

the security journal

*Manage your autumn business bounty...
and prepare for those cold winter months!*



Tips for TCP Testing

*IT Security Project Management...
A Syngress Book Excerpt*

Wargames 0x07D6

The SSN, Identification, and Authentication

*Phishing
Phundamentals and more...*



Volume 17 - Fall 2006 Edition



Your global information security experts

5350 Tomah Drive
Suite 3500
Colorado Springs, CO
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers
Assistant Editor: Michele Fincher

The Security Journal is always looking for quality writers for this publication. If you're interested in submitting an article for an upcoming edition, please contact us at editor@securityhorizon.com.

Interested in advertising in The Security Journal? Contact us at editor@securityhorizon.com

Special thanks go out to Ping Look from Look Designs for the creation of the Security Horizon logo and masthead images for The Security Journal.

For more information on Look Designs:
www.republicofping.com
design@republicofping.com

For more information on Security Horizon, please visit our web site or email us at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is headquartered in Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents

Notes from the Editor
russ rogers.....p. 3

IAM Course Schedule.....p. 4

Tips for TCP Testing
clinton smith.....p. 5

IEM Course Schedule.....p. 6

Syngress Publishing Book Excerpt
susan snedaker.....p. 8

Wargames 0x07D6
chuck little.....p. 13

Management's Role in a Successful Information Security Program
greg miles.....p. 18

Fundamental Problems of the SSN in Regards to Identification and Authentication
robert beken.....p. 21

They are Phishing for YOU
ed fuller.....p. 24



Copyright ©2006 by Security Horizon, Inc.
All rights reserved. Reproduction without permission is prohibited.



Black Hat[®]

Briefings & Training

Events for 2007

Black Hat Briefings & Training DC

Sheraton Crystal City • Arlington, Virginia

February 26-March 1

Call for Papers and Registration Opens October 1.

Black Hat Briefings & Training Europe

Movenpick • Amsterdam, the Netherlands

March 27-30

Call for Papers and Registration Opens November 1.

Black Hat Briefings & Training USA

Caesars Palace • Las Vegas, NV

July 28-August 2

Call for Papers and Registration Opens February 1.



Russ Rogers
CISSP
Editor in Chief

WOULD YOU LIKE TO BIGGIE SIZE THAT ACCESS?

allowing their users to run amok on their networks, and mitigate those concerns.

One of the core concepts of computer security is least privilege. Each professional in the industry has this concept drilled into their head. Least privilege basically states that a user should only have access to the data and/or resources needed to accomplish their job requirements. By limiting access to only what is needed, we also limit the risk of intentional or accidental damage to the critical information that keeps the organization alive.

.....

The United States is a nation of excess. We “value size” this and we “biggie size” that. We buy trucks that have more square footage than family homes in other countries. Our beds are bought and sold in terms of “King size” and “Queen size.” We even watch our 300+ cable and satellite television channels on 60” big screen television sets. The US has the 2nd largest military in the world, as of 2005; 2nd only to China (1). The irony here is that China has more than 4 times population of the US (2).

Don’t get me wrong, I like our way of life, even if I do believe we’re a bit excessive at times. But this culture of excess has created a dangerous mentality in the world of network computing. Users want to “biggie size” their access to the network and its resources. Maybe it’s a status thing. Maybe it’s just a case of “keeping up with the Joneses.” Regardless of what it stems from, companies have to understand the risks involved with

The executives, managers, and users of the organization should understand that the concept of least privilege does not automatically imply that we believe our employees are on some sort of vendetta to kill the organization. In most cases, we all want to believe the best about our employees. But as leaders in the organization, we also need to be absolutely clear about one thing, accidents happen.

Security Horizon has done work for more than one organization that has had a mishap caused by a well-intentioned developer who logged into a production server to make a minor tweak to the code. Despite the good intentions of the developer, the resulting outage causes a loss in revenue, a loss in availability of critical applications, or worse; a security flaw being introduced that results in the loss of sensitive customer information.

According to the 2006 CSI/FBI information security survey (3), 39% of respondents

Notes, cont.

who reported a financial loss due to security incidents said that up to 40% of those financial losses could be directly attributed to the insider threat. These statistics show a direct correlation between the actions of employees, either intentional or accidental, to negative financial results on the organization.

So the next time a user complains about what they can or can not access, consider your risks closely before you make a decision. Does the user need access to that service, application, or account? If not, is it worth the potential consequences to give it to them anyway?

In closing, I'd like to say thank you to all of our partners, customers, contributors, staff, sponsors, and readers. As we begin our fifth year of publication online, I attribute our success to the participation of all those parties involved with the Security Journal. Thank you!

I wish you all a very healthy and happy holiday season.

-Russ Rogers, CISSP, Editor



Errata:

Our last edition should have listed the authors of *The Security of Homophonic Data Encryption Standard* as G.Geetha and Dr. M. Thiyagarajan. Dr. Thiyagarajan may be reached at m_thiyagarajan@yahoo.com.



11/1 - 11/2, 2006 Gaithersburg, MD

11/6 - 11/7, 2006 Las Vegas, NV

11/13 - 11/14, 2006 Colorado Springs

1/16 - 1/17, 2007 Tempe, AZ

1/30 - 1/31, 2007 Fairfax, VA

2/6 - 2/7, 2007 Seattle, WA

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting, INFOSEC assessments of information systems using NSA's methodology. It is a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

FREE 1 Year license to the SAINT Vulnerability Scanner just for attending any of our courses!

**Training so good we teach
the competition!**

To register for one of these courses or to get further information, please contact us at:

(719) 488-4500

info@securityhorizon.com

<http://www.securityhorizon.com>



Overcoming Microsoft's Network Limitations



It is 4:00pm on a Friday afternoon. You have just spent the last 4 days profiling your network and your half-open portscan is running like an opiated greyhound. As a highly paid information security professional, you have better things to do with your time!

The root cause of the problem could be a security enhancement which was implemented with XP SP2 which limited the number of concurrent TCP connections to 10 (it was previously over 65,000).

problem?

A quick look in the windows event viewer (eventvwr.exe) will show events with an ID of 4226 which look like this:

EventID 4226: TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts

Well what can we do about this? Overcoming this issue has been addressed by a clever

...your half-open portscan is running like an opiated greyhound...

This limits not only the effectiveness of your PC to become a DDOS bot, but also its ability to perform any network activity with many open connections. The consequences of which will impact your ability to undertake portscans and other network assessment processes.

Unlike previous implementations which could be modified with simple registry changes, XP SP2 introduced modifications to the TCP.SYS file.

One way to overcome this problem is to use an alternate operating system, but for those amongst us who are UNIX-challenged, or who simply wish to use many of the Windows tools, I will outline a technique which can overcome this limitation.

So how do you know if you have this

fellow in Germany by the name of Markus Goslar. At his website you will find information about the problem and a useful patching utility which will patch the TCP.SYS file.

To ensure success, be sure to follow the documentation that comes with the patch and the on-screen prompts (as Windows attempts to prevent and/or undo what the patch implements). Another point to be aware of is to reinstall the patch after applying any changes to the TCP.SYS file; e.g. certain Windows updates.

Mr. Goslar's website can be found at <http://www.lvllord.de/?lang=en&url=news>

After running the patcher and a reboot, the problem should be resolved and you can again become the net-jedi you were born to be. (i.e. get your work done faster).

Tips for TCP Testing, cont.



A word of warning for those who like to aggressively SYN scan. Be aware that after making the above change, a fast or aggressive SYN scan with high connection numbers is a Denial of Service and is unlikely to ingratiate you with your masters or clients.

I hope you find this as useful as I have. Happy Scanning!



Clinton Smith currently holds a position with HBOS (Halifax Bank Of Scotland) Australia and is responsible for the management of IT Risk Australia-wide. He can be reached at Clinton.Smith@hbosa.com.au



We speak CVE®!

The INFOSEC Evaluation Methodology (IEM) is NSA's hands-on process for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture.

11/3 - 11/4, 2006	Gaithersburg, MD
11/8 - 11/9, 2006	Las Vegas, NV
11/16 - 11/17, 2006	Colorado Springs
1/18 - 1/19, 2007	Tempe, AZ
2/1 - 2/2, 2007	Fairfax, VA
2/8 - 2/9, 2007	Seattle, WA

To register for one of these courses or to get further information, please contact us at:

(719) 488-4500
info@securityhorizon.com
<http://www.securityhorizon.com>





Examine, expose, and exploit your vulnerabilities before an attacker does.



Introducing the first integrated vulnerability assessment and penetration testing tool. SAINTexploit™, developed by the maker of the award-winning SAINT scanner, gives you the ultimate resource to demonstrate the security—or vulnerability—of your network before an attacker gets there first.

SAINTexploit™ integrates seamlessly to:

- Examine potentially vulnerable services
- Expose points where an attacker could breach the network
- Exploit the vulnerability to prove its existence without a doubt

Don't just expose your vulnerabilities, exploit them.

To learn more, visit www.saintcorporation.com/saint_exploit.html or contact Billy Austin at 1-800-596-2006 x0119 or austin@saintcorporation.com.

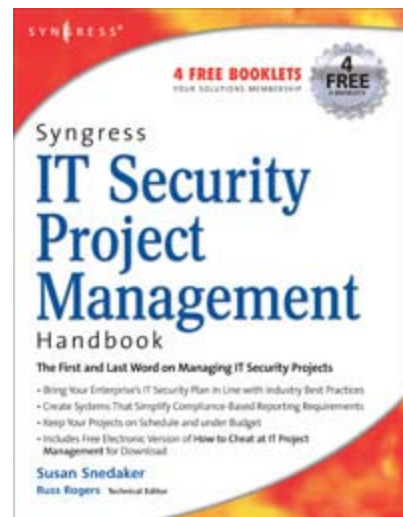
Book Excerpt: Syngress Publishing



The following is the first part of a two-part book excerpt from:

Syngress IT Security Project Management Handbook

by Susan Snedaker and featuring Russ Rogers, Technical Editor
ISBN: 1597490768



Chapter 4: Building Quality Into IT Security Projects

Solutions in this chapter:

- *Planning IT Security Project Quality*
- *Monitoring IT Security Project Quality*
- *Testing IT Security Project Quality*

Introduction

We often think of quality as something to check for in workmanship (e.g., whether a chair or a car is well-made). Quality in software projects is also easy to spot. A program that has few bugs and works as advertised is considered a higher quality product than one that keeps crashing or one that generates errors. When we think of Information Technology (IT) security, we typically think of secure versus vulnerable, protected versus unprotected, and safe versus at-risk. None of these really evoke thoughts of quality, but if you think about what will make a network secure, protected, and safe, it is the quality of several processes.

How well you perform your risk assessment will result in how well-protected your network ultimately is. How well you delineate the steps necessary to harden your servers or your

network infrastructure ultimately leads to how secure your network is. Quality should be at the forefront of your mind as you define, organize, plan, and manage your IT security project plans. In this chapter, we look at some of the elements you should address in your IT security project plans.

Quality and security have a lot of common traits. Just as with quality, security is difficult to quantify or recognize, because the measure of its success is the absence of failure. Much like insurance, you never want to have to use it, but unlike insurance, if you have your security systems in place, the expectation is zero failure, not 98 percent success. The quality of a security project plan seems more difficult to quantify, but if you do so, adding these measurements to your project will help you maintain the highest possible security standards.

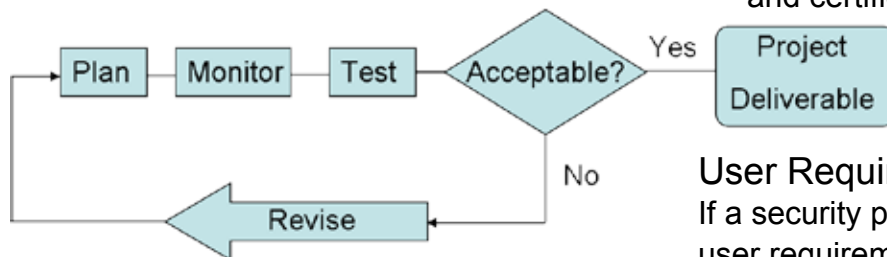
Planning IT Security Project Quality

Just as with standard project management, quality begins in the planning phases. Errors and omissions in the planning stage are amplified throughout the security project plan, and typically become very serious issues at

Book Excerpt: Syngress Publishing, cont.

the other end of the project lifecycle, in the implementation or maintenance phases. Planning is the first place quality is “built” into the security project plan, but as with all project management, it’s a continuous cycle (see Figure 4.1). The security project plan is created, implemented, monitored, and tested. Any changes are typically brought back through the project lifecycle as revisions through the change management process. Revisions are almost always necessary, as more detail becomes known through the planning process. As we plan, we understand the security project plan better and may revise the security project plan based on new data or a deeper understanding. In addition, we typically test our assumptions, create workflow models, and develop lab protocols. The results of these should feed back into the security project plan in a logical and thoughtful manner. This continuous loop helps create continuous improvement.

Figure 4.1 Quality Assurance Process



One word of caution: Don’t get caught up in the loop, and never deliver final results. You will have to draw a line at some point and deliver the final security project plan. One indication that you need to stop looping and start delivering is when you find that the revisions are becoming smaller and of less importance, or that you’ve refined the data to about an 80 to 90 percent level of accuracy or acceptability. You’ll most likely never reach 100 percent; shooting for it is one of the reasons people get locked in a feedback loop. You might also have key metrics that you define that indicate when it’s time to move

forward, or you might have a hard deadline that drives you to finalize your security project plan. Keep in mind that achieving higher and higher levels of quality when you’re nearing 100 percent becomes more difficult. It’s not a straight line increase between 95 percent and 96 percent, it’s an exponential increase. The time, effort, and cost associated with perfection is rarely practical, and you’ll need to assess your level of quality against your level of risk and determine when to stop revising and when to start working.

The following are specific areas of the planning process that directly impact quality:

- User requirements
- Functional requirements
- Technical requirements
- Acceptance criteria
- Quality metrics
- Change management procedures
- Standard operating procedures
- Federal or state laws, industry regulations, and certifications

User Requirements

If a security project plan fails to meet key user requirements, the project is essentially a failure. It’s sometimes easy to forget the fact that IT is a service provided to the company to facilitate, enable, and enhance its ability to get the job done. Business activities are performed by various company users, so it’s important to find a balance between pure IT security objectives and what users actually need. As discussed in Chapter 3, including key users into your IT planning process early in the lifecycle will help ensure that user needs are considered throughout. It’s easier to negotiate and find solutions to user objections or issues early on, than it is to go

Book Excerpt: Syngress Publishing, cont.

back through your security project planning steps and re-work a “perfect” IT security solution. The net result might not be the optimal one from an IT security standpoint, but if it meets corporate, IT, and user needs, you have a much better chance of successfully implementing and maintaining security.

Functional Requirements

Functional requirements are often derived directly from user requirements. Functional requirements describe how a system should perform, often from the user’s perspective. The system can be described or defined as any part of your IT security solution, such as user logon requirements or firewall functional requirements. Functional requirements are typically delineated as the services, tasks, or functions required of the system. To use a more concrete example, suppose you are defining the user logon process. The functional requirements might include the requirement that the user only has to log on once to access all information, or it might state that the user be required to logon additional times as they move across domains or into more confidential data. The functional requirements would define how that logon function should work, so that when the security solution is being developed, the IT staff can create the solution that fits these requirements.

Functional requirements are often tied to federal, state, or industry regulations, as well as certifications. For example, if you are working on a security project plan that includes the student health services on a local college campus, you must be compliant with a variety of regulations including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). (See Chapter 9 for more detailed information on some of the common regulations that might impact your IT security project plan.) Requirements that are

part of governmental or industry regulation typically have a precise and detailed list of specifications that your staff, processes, and technology must comply with in order to meet standards. Where available, these should be included as functional requirements. If the requirements are not clear or do not provide the set of detailed specifications necessary to meet certification or regulatory requirements, you’ll need to do a bit more research. In some cases, you may need to consult with industry or regulatory experts for clarification, or you may need to seek appropriate legal advice in order to ensure your IT security project plans deliver the requirements for federal, state, industry regulation, or certification.

Technical Requirements

The technical requirements are usually created after the functional requirements. Technical requirements are statements of parameters or measurements (e.g., the Transmission Control Protocol [TCP]/Internet Protocol [IP] ports that are required for various applications so that the firewall can be properly configured, the number of users a solution must support and the maximum amount of time it takes a user to login can be defined; and the minimum amount of disk space required for an Intrusion Detection System (IDS) can be configured.) These are all examples of technical requirements that should be included in your security project plan. As you can see, it usually makes sense to create your functional requirements to describe how your security systems should work, and then create your technical requirements. However, there may be times where you start with technical specifications because your system needs to meet very specific technical parameters. Keep in mind that most legal, financial, regulatory, and industry requirements begin as functional requirements, and must be translated into technical requirements in order to be

Book Excerpt: Syngress Publishing, cont.

incorporated into the security project plan (e.g., if you are required to protect personal information due to HIPAA, you should build those requirements into your functional and technical requirements as well as into your acceptance criteria).

Business Intelligence...

Functional Requirements Can Help Reduce Complex Security Challenges

Storage Area Networks (SAN) are complex devices that are used by many network entities, from servers to users to applications, and beyond. Using functional requirements can help you reduce the complexity so that rather than trying to wrap your arms around the entire universe of users, you can look at the required functionality. In this way, you can look at the functional areas to determine how the SAN security system should work. An article that appeared on the Search Security Web site in December 2005, describes the five A's of SAN security as authentication, access, auditing, alarms, and availability. Approaching SAN security from these functional areas allows you to work through your security project plan in a methodical manner. Once your functional requirements are defined, you can move into defining the technical requirements. (For more information on the five A's article, go to http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1152494,00.html.)

or an individual project deliverable will be accepted. In some project management situations, acceptance criteria are the measurements by which the security project plan is accepted and paid for; therefore, these metrics can literally mean the difference between profit and loss. With internal projects, there usually isn't the issue of whether or not you'll get paid; the issue is whether or not the security project plan will be deemed completed and successful. At some point in our careers, most of us have been in a situation where it almost feels like a pair of six-year-olds quipping back and forth, "Did too!" and "Did not!" This is the kind of situation you would always prefer to avoid rather than repair, and the best way to do that is through acceptance criteria.

By definition, acceptance criteria are "pre-established standards or requirements that a project must meet." When you define these at the outset of the security project plan, you can get all of the relevant stakeholders on the same page and agreeing to the same results. Referring back to the user example: Suppose the Accounting department wants users to have to login a second time to examine specific documents, but the Sales department wants one fast, easy way for its remote sales people to login to the network and retrieve accounting documents, sometimes over intermittent or slow connections. If you appease one group, you'll likely frustrate the other. In this case, you'll end up with a security project plan that is deemed a failure (or at least, less than successful) by one group or the other. To avoid this kind of push-pull, define requirements and acceptance criteria for each of your individual security area project plans, as well as for your security project plan as a whole. Make special note of any legal, financial, regulatory, or industry requirements that must be met, and build them into your acceptance criteria.

Acceptance Criteria

It's always a good idea to define the criteria by which a security project plan as a whole

Book Excerpt: Syngress Publishing, cont.

Quality Metrics

Specific quality metrics may be difficult to define for your security project plan because, as stated at the outset of this chapter, the definition of quality is “the complete absence of incidents.” If your network is targeted by hackers and they fail to get in, you have achieved a quality result. While you and your IT staff understand the enormity of that result, it’s entirely possible that those outside of the IT world see it as a non-event. In reality, it is the compilation of non-events that proves that your security solution delivered the requisite level of quality.

Still, there are ways to define quality. For instance, when implementing intrusion prevention and intrusion detection systems, you want 100 percent prevention and zero percent intrusion. Is this a reasonable and achievable metric? It would seem so since even one intrusion could cost your company millions of dollars, thousands of hours, and untold cost to the company’s reputation. Therefore, you should consider creating quality metrics to the highest degree possible. Even if you have difficulty quantifying these metrics, making the effort will help keep you and your IT security team focused on quality. However, let’s remember that quality has to do with errors and defects. Even if you have zero errors or defects, a network intrusion can still occur for other reasons; therefore, you need to define the level of errors or defects that are acceptable. While most everyone would agree that zero is the best, it’s usually not an achievable metric. You will have to balance your time and budget against your quality metrics to make sure you’re delivering a reasonable solution. If you wait until it’s perfect, you will never implement anything. Be clear about where you’re drawing the line and why. Document what exposure these choices might create, and the decision-making process that you used to balance the time and cost against results, so that you have

a clear record of this process that you can refer back to later, or that you can provide to management should you be asked.

As discussed previously, quality needs to be balanced against the constraints of the security project plan. For example, to meet the requirement of 100 percent prevention of intrusion, you might have to spend twice as much as is in your budget. On the other hand, you might be able to achieve 95 percent prevention within your budget. The cost also has to be counterbalanced with the amount of risk your company is willing to accept, as well as the value of the data being protected. This equation is critical to understanding and addressing the cost of security. The acceptable level of risk and the value of the data being protected should be kept in mind throughout your IT security project planning process.

In many cases, quality is not a discrete deliverable, but rather a mindset and a cultural attitude. When you focus on quality in your IT security project plan, you are sending a message to the team and the company that quality is critical to the success of the project. Defining and quantifying it in ways appropriate to your specific security project plan is a worthwhile endeavor. You might be surprised at how you and your team can define quality within the framework of an IT security project plan.



~ Look for Part 2 in our next edition ~

Syngress Publishing (www.syngress.com), headquartered in Rockland, Massachusetts, is an independent publisher of print and electronic reference materials for Information Technology professionals seeking skill enhancement and career advancement. For more information on Syngress products, contact Amy Pedersen at 781-681-5151 or email amy@syngress.com.

(a.k.a Capture The Flag 2006)

For the DC303 crew, preparation for Capture The Flag 2006 began soon after Dark Tangent closed DefCon 2005. Well, preparations didn't begin quite that soon, but planning and the initial gathering of interested parties did. Plus there were the unenviable hangovers to still be dealt with; the last remnants of the previous evening's 303 party. Regardless, we were all pretty psyched up to compete. Little did we know what we were getting ourselves into <insert evil laugh>.

The Capture the Flag competition generates so much interest that a qualification round is required to whittle the list of teams down to a manageable number. The qualification round took place the weekend of June 9th, and

keeping with the team name, "our wives are pissed", my wife was not happy. I had forgotten to remind her about the CTF qualification round being that weekend (Sorry Karmen!), and that I would be gone almost the entire duration of qualification round/ weekend. Fear not, trusty readers, for I am back in her good graces...flowers and a card can do wonders. *smile*

Anyway, back to the CTF qualifications. There were 116 teams competing for 7 spots; to be one of the 7 teams to compete against last years CTF winning team (for a total of 8 teams). A Jeopardy-like scoreboard was used for the qualifications, each team had from Friday 10:00pm EST to Sunday 11:59pm EST to answer as many questions correctly as possible (see the below screen capture showing the scoreboard. Credit: drb@nopsr.us). There were five categories, with five

CTF Quals 2006

Score: 6400

Potent Pwnables	Binary Leetness	Forensics	Web 3.0	Trivia
100¥	100¥	100¥	100¥	100¥
200¥	200¥	200¥	200¥	200¥
300¥	300¥	300¥	300¥	300¥
400¥	400¥	400¥	400¥	400¥
500¥	500¥	500¥	500¥	500¥

YOU'VE GOT NUTS!!1!one!1 Double word score... This question gives you 500 points for clicking. If you give up, you keep the initial 500 and lose the question's 500 (break even). If you answer correctly you get the additional 500 points (for 1000 total.) (The server is at kenshoto.allyourboxarebelongto.us.)

Files

I owned it It owned me

Leaders

1. Sk3wl0fR00t (7500)
2. Digital Revelation (6500)
3. 1@stPlace (6400)
4. fednaught (6000)
5. Pangolin (5900)
6. Fast (5600)
7. our wives are pissed (4800)
8. WCSC (4000)
9. Guard@MyLANO (3500)
10. PARADOX (3400)

levels of questions/tasks in each category; values were 100 to 500 points. The categories were: Binary L33tness, Web Hacking, Potent Pwnables, Forensics, and Trivia.

- Binary L33tness category primarily dealt with reverse engineering.
- Web Hacking category was exactly that, hacking web sites that Kenshoto had put together for the competition. All sites were hosted at `kenshoto.alloyourboxarebelongto.us`.
- Potent Pwnables category was focused on remote exploitation; and they may or may not provide binaries for analysis.
- Forensics category dealt with...wait for it... wait for it (trying to keep you guessing)... forensics. Time to put that high-speed, low-drag, SANS forensics training to use.
- Trivia category was described by Kenshoto as "Know your profession / hobby. Random useless facts we arbitrarily deemed important enough for you to know." Pretty vague, huh? :) But it was a cool category.

Just as in Jeopardy, if you answer the question correctly, you get the points that the question was worth. If you answer incorrectly, you lose that amount of points. I won't go into a detailed, or even cursory discussion of the questions since a complete list of all the questions and answers for the CTF 06 qualification round can be found at <http://nopsr.us/ctf2006prequal/>. The site has the associated binaries available, as well as a walk-through of each of the categories' questions and answers.

Well, to make a long story (weekend) short, the team ended up placing 7th, which got us in to the CTF competition. We had hoped to do better, but at least we made it! But then the reality set in: CTF/DefCon was less than 2 months away. Time to get mah' learn on. So we could start focusing our preparations,

we asked Kenshoto what OS we would be defending/attacking for the CTF competition, but they wouldn't do any more than drop hints as to what the OS would be. When our team lead, Mantis, asked Kenshoto what the OS would be, the answer on the MUD basically was that we got a brief taste of the favored OS and programming language we would be expected to defend/attack/all-that-jazz for CTF '06. Since most of the binaries were FreeBSD, that's the OS we thought we would be using for the competition. Boy, were we wrong. We got the programming language correct, Python, but not the OS.

Jump ahead to DefCon/CTF weekend. The team has been practicing reversing, disassembly, python programming, and defense of FreeBSD. We are ready. We've been studying, and hacking, and defending (operating systems, not court cases) for the past couple of months. It's time to put all of that hard work to the test. The competition start was delayed due to the start of DefCon being delayed by two hours. But soon Kenshoto called all the team leads up for a kick-off meeting. I took one look at our team lead's (Mantis) face when he was walking back towards our table, and knew that a monkey wrench had been thrown into the works. Mantis said "The OS is...Solaris 10 x86." Our jaws dropped. But, but, but...that's not the operating system we thought we were going to be attacking/defending! We weren't ready for Solaris 10 x86, we were ready for FreeBSD (any version)! <again with the evil laugh... where is it coming from?!?>

Kenshoto had the team systems set up in Solaris Containers (Zones), and each team was assigned a subnet (e.g. 192.168.7.0/24) for their use. The team's server and gateway were each assigned addresses from this range as well. And since all traffic was source NAT'd, we couldn't distinguish between

valid traffic (e.g. Kenshoto service level monitoring), or attacks from opposing teams. No firewall, no IP filtering, and (at least initially) no network sniffer available. We had to defend a server we couldn't protect, or monitor. To quote my teammate Syndrom, "Awesome!" (I hope everyone picked up on the obvious sarcasm. *smile*) Additionally, our services up-time contributed and/or detracted from our overall score. So add to the mix that we had to keep these very vulnerable services running, or have it detract from our score. But if the services are running, then we start "leaking keys like a sieve." Keys (or tokens), which the teams get points for stealing, pwning, and overwriting, were the primary means of scoring in CTF '06. Though, I must add that the service level was way more important than we initially thought. It was used as a multiplier for all the other categories. The teams received points, or were penalized points, in the following categories:

- **BT:** Break Throughs. In this category you received points for discovering new vulnerabilities (on the team systems), and submitting a write-up of the vulnerability, how to exploit it, etc. Teams were only awarded credit for the submitted Break Through write-up if the break through gave access to a private key or allow for an overwrite of a key.
- **Steals:** This is how many keys the team has stolen from the other teams. The keys are stolen by exploiting one of many vulnerable services, and obtaining the private key that the service contains.
- **Pwns:** To score in this category, the team must exploit one of the vulnerable services, and overwrite the service's key, with their team key. Kenshoto monitored all the key locations and automatically recorded when a "key overwrite" occurred
- **Penalty:** You don't want any score in this category. Teams were penalized if they intentionally DoS'd other team servers/services, if you had more than 10 team members at your table, things of that nature.

- **SL:** This is the Service Level category. Teams were rated on the availability of the services they had to defend. Kenshoto monitored the availability of all the teams' services, and tracked SL uptime percentage. The SL percentage was based on the number of successful (service) polls divided by the total number of (service) polls. Everyone starts at 100% in the SL category, and it goes down from there.

There were three types of keys as well: Public, Private, and Overwritten. A public key is exactly that, it's public and normally visible. A public key can be overwritten and get you points that way. A private key is not normally visible, but if you compromise the associated service then you could obtain the private key and thus score. Some private keys were also over-writable. An overwritten key is one where an opposing team has compromised a service and overwritten that team's service key with their own team key, thus scoring points. The competition was broken out into "scoring phases", and Kenshoto would update the private keys during each scoring phase. This meant you could get many unique keys (score!) by repeatedly stealing keys from vulnerable services/teams.

To submit keys for scoring (keys you have stolen from other teams), Kenshoto provided an analog line to their Asterisk server. Via this phone line, you could ring up the other teams, check voicemail, or connect to the "Hotline." Through the Hotline, you could check the team Service Level status (provides status on each service as "up" or "down"), submit keys, or submit Break Throughs. Additionally you could check the status of Break Throughs submitted.

The final score was computed by adding up the BT values (assigned by Kenshoto), Steals, and Pwns, then multiply that by the Service Level, and finally subtract any Penalties. After the competition was over, and the scores tallied, team "our wives are pissed" ended up

in 5th place overall. We dropped from 4th on the leader board; probably due to Break Through scoring and Service Level scoring adjustment.

All in all, it was a phenomenal weekend. I didn't get to attend any DefCon presentations, but I learned more this year than any other year I have attended the conference. Now that we know the stakes, and what it takes to win, we will be better prepared for next year. So be forewarned fellow Capture the Flag'ers, Team "our wives are pissed" will be playing

(and initially had no idea what was going on).

I'd also like to thank the folks from Kenshoto, and the other CTF '06 teams. I learned *A Lot*, and I'm sure the rest of the team did as well, from these fantastic folks. And I must say it was rather humbling (at least for me). It may sound corny, but it was an honor competing in CTF. I've wanted to compete in CTF since the competition started, but I never have. I didn't think that I had the skills to compete at the level required for the CTF competition. But now I know differently. Now I know what is

required to compete, nay, win the Capture The Flag competition: adaptability. One can go into the competition knowing all the OP codes for every processor, able to disassemble binaries with a single thought, able to perform SQL injections with a wave of his/her hand, etc. But if that person cannot adapt to the environment Kenshoto throws at them, and adapt their knowledge and skills so they can wrap their head

	BTs	Steals	Pwns	Penlty	SL
1stPlace	6	1281	207	0	93%
fednaught	5	717	557	0	81%
Shellphish	9	868	133	0	84%
our wives are pissed	4	553	245	0	91%
Sk3wIDIR00t	7	569	199	0	76%
TheEastSea	1	178	0	0	67%
Digital Revelation	4	18	11	0	50%
Ad Hoc	1	53	2	2	22%

00:01:08

Congratulations on not up the network - Put Kev

for keeps next year. The wives may not be pissed (at least we hope not), but the team will be there with the same drive that got us to 2nd place and kept us there for most of Saturday. Armed with the additional skills we will be gaining throughout the coming year, and knowledge of what it takes to win, I say we will be a force to be reckoned with.

On a personal note, I would like to thank and congratulate team "our wives are pissed." I learned the most from my teammates, and was inspired to learn even more just so I could contribute to the team's success. Everyone on our team contributed where they could, and I think we did pretty good, considering it was our first showing at CTF

around the screwy Python binaries Kenshoto wrote for the competition, then they won't make it. Well, we are going to make it.

Thanks to Doc Brown (drb@nopsr.us) and team 1@stPlace for the excellent CTF '06 write-ups, which I referenced, and pictures, which you see here.



Chuck Little is a security consultant for Security Horizon, Inc. He may be reached at chuck@securityhorizon.com.

The Future

Brought To You By Inspiration—and Coffee

The University of Advancing Technology (UAT) provides students a diverse, exhilarating environment where the best elements of a college education collide with an unrivaled passion for advancing technology. It's an innovative educational model that gives talented individuals an opportunity to create the future with a complete immersion in the rapidly expanding technological universe. We need the very best professors/instructors to continue this vision. If you are committed to expanding the field of technology (online or on-campus) through research and sharing of knowledge—challenging, educating and empowering students, we invite you to explore the teaching opportunities at UAT.



Learn more.

www.uat.edu or email Dave Bolman,
Provost at dbolman@uat.edu



...in a Successful Information Security Program



Who are the Managers Here?

In every organization there are individuals, or groups of individuals, that have the responsibility and hopefully empowerment to make decisions that affect the organization. These decisions can be based around how to market products/services, how to effectively accomplish a mission, or better serve their customers. The bottom-line commonality is that they make decisions that affect the organizations operations, funding, and success. For the purpose of this article, we are most interested in the decisions they make concerning information security and risk.

Risk

Businesses everyday must consider RISK. Risk to their business and risk to their bottom line. We call this business risk. Closely related to this is security risk. Security risk can be defined as the combined effect of threats, vulnerabilities, and impact to the organization. Managers play a critical role in the risk management process, especially when you consider how closely business risk and security risk are tied together. The decisions they make will have a direct impact on the overall risk to an organization.

Management Buy-in

In the security industry we talk a great deal about the importance of management supporting the security efforts we are attempting to put in place. This support is often referred to as "*management buy-in*". Management plays a psychological role in how an organization functions and implements programs. If management shows something is important, generally others in the organization will pick up on this support and it will be easier to implement improvements or in our case, better security.

Are all managers the same? Absolutely NOT!. Each manager brings a unique set of experiences to the positions they hold. Some are easy to work with and some not so much. Especially in security consulting, security can be seen as a nuisance or even worse, a confrontational area. I read an article recently that had the CIO in a defensive mode because the security guy (who worked for CIO) was identifying vulnerabilities in the organization. The CIO thought the security guy was out to get him fired. The CIO was not educated or informed of the purpose of the work that was going on. In most cases, security is not focused on finding fault, but in finding ways to improve security posture and therefore reducing business risk. Of course this is a case for conflict of interest, but that is a discussion for another time.

I believe we all understand management support is important, but how do we get management to support the process?

How Do You Gain Management Buy-in

Getting management support for your security program involves understanding both the culture of the organization and the manager themselves. The organizational understanding will be driven by understanding the mission, customers, operations, critical information, critical systems, and industry specific requirements and constraints. Understanding the manager can be much more difficult. This understanding will be driven by the individual manager's personality, biases, experiences, work/life philosophy, and ability to work with others. Since we are trying to get management to support our security efforts, the best approach is a non-confrontational approach that will involve education, developing business cases, and developing compliance cases for having a quality security program within the organization.

Education: Educating management on the purpose and importance of security within the organization is one approach to gaining management buy-in. Don't expect this education to make the manager a security expert. But the education can show the manager how security can fit into the organization as a business support mechanism instead of the pre-conceived nuisance that it may be considered. Different types of managers may need different types of education. A technical manager may be able to handle more detailed security training than a non-technical manager. The technical manager, in fact, may expect a higher level of detail. This goes along with understanding the individual manager and their role within the organization.

Show Business Case: Many managers need to see information in the form of a business case. Considerations for security are no different. In my experience with

security consulting, business cases come in two major forms: return on investment (ROI) or cost avoidance.

Return on Investment Analysis: ROI analysis focuses on analyzing the resulting benefit (generally financial) from an investment of time or money into the security for the organization. It can be very challenging to show a financial return to an organization through supporting the security program. One exception I have experienced is in the area of insurance. We were asked to conduct an assessment of an organization to determine what would be required for them to meet their insurance company's information security requirements for reduced rates. Through investing approximately \$30,000 into their security program, this organization was able to save over \$100,000 in insurance premiums. This has a direct ROI of \$70,000.

Cost Avoidance Analysis: Cost avoidance is different than ROI in that it looks at costs that do not have to be paid by the organization instead of a return on the funds invested. Cost avoidance is easier to identify with security because the majority of security implementations are for the purpose of prevention. This analysis looks at what is most likely to occur, what is the associated cost should it happen, and how much time and resources have to be spent to keep something bad from happening.

Show a Compliance Case: Compliance concerns are becoming a big driver in information security. Regardless of interest in ROI or Cost Avoidance, most managers are concerned about whether they are compliant with relevant laws and regulations that they are required to follow. The CIO that was concerned the security person was out to get him fired, should have been more interested in the fact that the work the security

Management's Role..., cont.

person was doing would ultimately help the organization pass the associated audits.

What If I Fail?

There is no 100% guaranteed way to get management to support the security effort. If you have followed a reasonable approach to getting management buy-in and management still will not back the security program, then it may be time to consider moving on to other things. Recognize there will be some organizations and some managers that just will not understand the importance of security or they just cannot culturally or financially support what you consider a reasonable level of effort for security. Just make your best effort.

If you are a manager or decision maker for information security, listen to what you staff or consultants have to say about security. Take security into account when making your risk based decisions. And you too just need to make your best effort.

Management Buy-Out

Be cautious how you approach getting management support. FUD (fear, uncertainty, and doubt) is an overused approach to try to convince management to take action. There may be appropriate times to utilize FUD, but the real support will come from the other approaches mentioned above. Don't lose management support through trying to scare them.



Greg Miles is the President of Security Horizon, Inc. and a professor with the University of Advancing Technology. (www.uat.edu) You may contact him at greg@securityhorizon.com.



Your global information security experts

Advertisers!

Reach *THOUSANDS* of readers every quarter at an *outrageously low price!!*

The *Security Journal* is never offline, making your ad constantly available--ALL of our issues are still downloaded quarterly



Contact us at:
editor@securityhorizon.com
or
719-488-4500

the Social Security Number in Regards to Identification and Authentication



Not long after the Social Security Number's creation, it has been found to be an increasingly useful way of identifying persons, especially for computer systems. Social Security numbers are unique to individuals, and are not reused after one dies. The Social Security Administration has issued over 420 million SSNs since 1936, increasing at a rate of about 5 million each year. The administration doesn't expect to run out under the current numbering system for several generations to come.

This looks, at first glance, as the perfect way to identify people on a particularized basis; therefore avoiding the problem of thousands of people with the same name and birth date in the United States. It has, as we all know, become the de facto standard in identifying individuals in the United States.

Identification and Authentication mechanisms, human or otherwise, consist of: something you know, something you are, and something you have. Most computer based systems use one or two of these three factors, whereas other secure authentication systems use all three. Identification and authentication in the real world happens all the time, such as when you receive a phone call from someone you know.

1. Cell phone rings - Caller ID – identifies caller as “Steve” with a phone number 212-367-5309.
2. Request for authentication
3. Authentication

When Alice's friend Steve calls her, her phone rings and, these days, prompts her with the caller's identity “Steve” or his personal phone number. Alice recognizes this, answers the phone and says “hello”, prompting for authentication. Steve replies with “Hi Alice, it's Steve...” Alice recognizes Steve's voice and Steve is authenticated biometrically (We authenticate each other all the time. Think about it; face recognition, voice recognition, someone's mannerisms are all forms of human biometric authenticators. That's why there's a picture of you on your drivers license and passport).

Computer systems work the same way. When you log into your computer, you enter your userID or identification (the computer happily echos it back to you on the screen) which is not secure, and a password which is hidden, and something that nobody else knows, not even the administrator.

Back to our Social Security Number: older Social Security cards, in fact, used to be printed with the caption “Not for Identification”. Regrettably, not only is the social security number used every day as a means of identification, but also used as a means of authentication. In the recent HP spy scandal, HP's Chairwoman hired investigators to collect phone records of board members. Mr. Tom Perkins, who was asked to resign from the HP board, wrote a letter to the HP directors. In his letter, he refers to an occurrence where AT&T used the last 4 digits of his social security number “as a means

of authentication by an impersonator”.

This situation, unfortunately, is not a lone incident involving one particular company. A large number of major corporations (utility companies, large banks, and the like) and government agencies use Social Security Numbers as a means of authentication. Every time someone asks for your SSN (at the DMV, banking via telephone, your “last four” requested from your wireless carrier... the list goes on), think about it. Of course, everyone reading this article has eliminated such situations at *their* respective organizations... right?

The constant use of Social Security Numbers as a means of identification creates larger risk exposure for the owners. It is more

state of California to be notified in the event of data loss. This does not guarantee that every organization or company notices they have been hacked and data has been stolen, if the hacker knows what they’re doing.

Many prominent security experts have agreed that the use of the “social” has presented the largest challenge to computer privacy in recent years. The implementation of SSNs for authentication purposes is completely flawed. It is a fundamental issue to solve, but it is such a pervasive problem that it demands attention. As security professionals, we must evaluate the risks and threats of using SSNs in our systems, not only to our organizations, but to the individual as well.



specifically a privacy issue combined with the threat of identity theft to the respective owners of those numbers, rather than the company or organization that holds them. SSNs are used as a “primary key” across a large number of systems in use today. The advent of regulations such as SB 1386 requires organizations with customers in the

Robert Beken is a Security Consultant for a Fortune 500 organization and may be reached by emailing editor@securityhorizon.com



In this article, we'll discuss two common forms of fraud occurring on the Internet; Phishing and Pharming. Both are costing Internet users and companies billions of dollars every year through identity theft. While most people are aware of the Nigerian Internet email frauds there needs to be greater attention given to the Phishing and Pharming that is growing on the Internet.

Phishing is a social engineering technique accomplished via the Internet by sending an email message to a user claiming to represent a legitimate company that they do business with via the Internet. The goal is to trick the user into visiting a fraudulent website and disclosing sensitive personal information that would then be used to commit identity theft. Phishing is a play on the word, "fishing," since the phisher is putting out bait in the hope that some people will be suckered into responding to the message.

The Anti-Phishing Working Group (APWG) <<http://www.antiphishing.org/>>, an industry-sponsored association, received 23,670 reports of phishing for the month of July 2006 compared to 14,135 reports for July 2005. APWG estimates 75 million to 150 million phishing emails are sent daily <<http://www.antiphishing.org/APWG-FDICCommentaryLetter.doc>>. While most of these spam emails are blocked by spam filters and never reach corporate Internet users, it is estimated that a well-designed phishing email campaign can get response rates of up to 5 percent or over 3 million responses.

Phishers most often choose to target large financial institutions that have a large online customer base. The phishers will send the emails out to a broad base of user addresses. They have no idea if the recipient is a customer of the financial institution. This is done with the knowledge that a certain percentage of the email message recipients will be actual customers of that institution, and will likely believe the message is legitimate. Normally, the message presents some negative consequence to not responding to the email, such as an account lockout or the user being unable to conduct normal business. This is not limited to only financial institutions. Websites belonging to Internet service providers (ISPs), retailers, and even government agencies have also been targeted.

Once the user has contacted the fraudulent website, usually by clicking a link in the email, they are asked to provide or update personal information, such as credit card or bank account number, account username, password, security code, Social Security number, or any other sensitive personal information that is already held by the legitimate organization. Once the phisher has collected the information, they will normally sell the information via the Internet to others who intend to commit further fraud and or theft. With the victim's personal information compromised, the risk of a number of possible frauds exists such as:

- The information can be used to access existing financial accounts.
- The information can be used to apply for credit and open new accounts in the victim's name.
- The information can be used to hijack the victim's computer and use it as a platform to disseminate phishing and spam email messages to others.

- An increase in Phishing Attacks

These phishing websites are only online for a relatively short period of time. According to the APWG report < http://www.antiphishing.org/reports/apwg_report_july_2006.pdf >, the average time a phishing site remained active during July 2006 was 4.8 days and the maximum time online for a site was 31 days. The top 10 countries identified as hosting phishing websites was lead by the United States with 30% and the nearest competitor being the Republic of Korea with 13%. The remaining top 8 hosting countries were; China (12%), France (6%), Australia (5%), Germany (3%), Japan (3%), Canada (2%), Thailand (2%), and Italy (2%), accounting for 78% of all identified phishing websites.

There is a new variation of phishing that has emerged since 2003, Pharming. Pharming is a play on the word, "farming," since the pharmer is planting seeds in the hope that some people will be suckered into providing a crop by responding to the message. Pharming does not rely on social engineering to accomplish their objective. Instead pharming is done via malware or covert downloading. The goal is to infect the user computer when they visit a fraudulent or malicious website without any or very limited user interaction. When the user visits the website they covertly install a Trojan horse program such as a keylogger, backdoor, adware or spyware that will track the user's Internet or computer activity.

This information is then sent usually via Internet Relay Chat (IRC) to the pharmer who would then use the information to commit identity theft, or even login and take control of the user's computer. While the most common websites identified in pharming are pornography and game-cracking sites, this method can easily be used by phishing sites

or any other website that the pharmer can install code on.

Unlike most malware, phishing-based malware applications have tracking components, which attempt to monitor specific actions or targeted organizations, such as financial institutions, online retailers, and ecommerce merchants in order to target specific information. The most common are: access to financial based websites, ecommerce sites, and web-based mail sites.

There are basic defenses against such phishing activities. A U.S. Department of Justice special report < <http://www.usdoj.gov/criminal/fraud/Phishing.pdf> > recommends three simple rules to follow:

1. **Stop.** Phishers typically include upsetting or exciting (but false) statements in their emails with one purpose in mind. They want people to react immediately to that false information by clicking on the link provided and inputting the requested data before they take time to think through what they are doing. Users need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the e-mail may be. There is always enough time to check out the information more closely.

2. **Look.** Internet users should look more closely at the claims made in the e-mail, think about whether those claims make sense, and be highly suspicious if the e-mail asks for numerous items of their personal information such as account numbers, usernames, or passwords. For example:

- If the e-mail indicates that it comes from a bank or other financial institution where you have a bank or credit-card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate banks and financial

institutions already have their customers' account numbers in their records. Even if the e-mail says a customer's account is being terminated, the real bank or financial institution will still have that customer's account number and identifying information.

- If the e-mail says that you have won a prize or are entitled to receive some special "deal," but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize don't ask you for extensive amounts of personal and financial information before you're entitled to receive it.

3. **Call.** If the e-mail or website purports to be from a legitimate company or financial institution, Internet users should call or e-mail that company directly and ask whether the e-mail or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit-card accountholders can call the toll-free customer numbers on the backs of their cards, and bank customers can call the telephone numbers on their bank statements.

If you believe that you may be a victim of phishing, you should immediately file an online complaint with the Internet Crime Complaint Center (a joint project of the FBI and the National White Collar Crime Center) at <http://www.ic3.gov>. Because the disclosure of personal information may put you at risk of becoming a victim of identity theft, you also should go to the Federal Trade Commission's identity theft website, at <http://www.consumer.gov/idtheft>, and follow the directions there for reporting information to credit bureaus, credit-card companies, and law enforcement. If you have received a possible phishing e-mail, but have not yet responded to it, do not respond. Instead, send copies of the e-mail to the Federal Trade Commission (FTC) at [\[ftc.gov\]\(http://ftc.gov\) and the Anti-Phishing Working Group \(APWG\) at \[reportphishing@antiphishing.org\]\(mailto:reportphishing@antiphishing.org\).](mailto:uce@</p></div><div data-bbox=)

With an estimated loss of over \$50 billion per year being reported by the FTC <<http://www.ftc.gov/os/2003/09/synovaterreport.pdf>> and millions of consumers being victimized by identity theft each year, phishing represents a rapidly growing problem. Users need to understand that putting personal information out on the Internet places them at risk for identity theft. While users can limit their chances of being victimized by not responding to suspicious email messages, phishers will continue to use new strategies, such as Instant Messaging popup requests and installing spyware, to lure victims into giving out sensitive personal information. Phishing techniques will use any possible communication channel to socially engineer their desired illegal access to financial accounts or other sensitive information.



Ed Fuller is the Chief Operating Officer and Senior VP of Security Horizon. He has over 30 years of experience in Operations, Communications, Computer Information Systems and Security. He is the primary lead for INFOSEC Assessments, Appraisals and Training for Security Horizon. He may be reached at ed@securityhorizon.com