Global Information Assurance Certification Paper

Making it Real

Getting the right kind of attention when pointing out corporate security vulnerabilities

GSEC Practical
Version 1.4, Option 2
Michael Eisenstein

Abstract

There are plenty of hackers with the right intentions. Locate the vulnerabilities and then either fix them or get the people responsible for them to fix them. This paper touches on the ongoing debate of Good-Samaritan hacking, and delves into alternative methods of "making it real" to the people responsible for allocating resources.

Case One is an example of several small vulnerabilities on a corporate intranet leading ultimately to very high risk, and the method I used to point this out to management without actually hacking to prove the vulnerabilities.

Case Two covers a different sort of situation. In Case Two, significant financial loss was highly unlikely, but there was a large perceived breach of trust. It is an example of fighting a "not my problem" philosophy with patience and tenacity. It is a story of unintentionally intercepted instant messages.

Introduction

In many industries, managers can move up through the ranks (with or without a change of company) and maintain an understanding of the details of the jobs from which they graduated. The higher one gets in the management chain, the less one has time to learn the details of each operation under one's command as those operations change with technology. This applies to database administration, desktop support, and certainly security. A review of online resources leads to a surprising discovery: there is no publicized training for managers on network security issues. As of this writing, even SANS has a course named for, but no instances of training for management relating to security. SANS training for techies covers how to take security issues to managers in some depth, but it is still difficult to make security *important* to managers.

Case One – Feeling Virtual Pain

Presented in Case One is an example of one method of "making it real" to management without hacking systems, unlike most Good Samaritan hackers who simply break in to make a point.

Introduction: Hackers Don't Do What They Are Expected To Do

Security by obscurity is not security at all. For most people or organizations outside of banking/finance, energy, government, or military, it is easy to believe that no hacker really cares about them. After all, what kind of damage can a hacker do to a site that doesn't take orders, doesn't have credit card or customer information in a connected database, doesn't get a million hits a day, or has no sensitive information? This comes from a lack of understanding of the hacker community. This loose, semi-anonymous subculture has created its own ideas of honor, style, credibility, and ideals, especially in the definitions of concepts like "cool" or "impressive". White hat security people, law enforcement, and the average computer users consider them vagabonds, crooks, vandals, or idiots. The hackers themselves can live virtually in a community where larger exploits may garner greater accolades, but any exploit is part of a seasoning process that takes a nobody and turns them into a known name in their community. Perhaps it could be compared to gang membership, where some tests must be passed to prove a novice's mettle. And in addition to these people fully enveloped in the hacker society, there are people who just like to test the waters. One SANS student expressed it best:

> "Ok, now I have all my tools for hacking a Unix system, all I need to do now is find a place that I want to hack in to and go for it. Given that I am new I will probably start small. I'll find some small company that has a weak security system, as they cannot afford a top of the line administrator and all the relevant tools, and I'll practice on their system."[1]

While he may not have actually cracked any systems, he clearly showed that small companies are targets *because of*, and not despite their size. There is no security in obscurity.

[1] Lisman, Jarrad, P 4

Merely explaining to a senior manager that being small does not make you an invisible target does not generally get management to start pouring money and time into securing their systems. It is very likely that management is not aware of the attacks on companies smaller than an eBay or Yahoo!. "Computer crime experts have long believed that computer-related offenses are drastically under-reported…. Some victims are reluctant to come forth, because they … are embarrassed by their vulnerabilities, and will take strong measures to avoid any publicity"[2]

Before – The Unevaluated Risk

In April of 2001, I worked for a high tech company. This meant working around many people with a good understanding of computer and network security. Unfortunately, our IT staff had some combination of the following:

- A poor understanding of security.
- Inadequate time or resources to implement good security.
- A lack of understanding of what sensitive data could be exposed.
- Simply too much trust in people, and therefore the assumption that holes would not be exploited.
- The assumption that our company was too small a target for an industrial spy to bother with.

By April '01, I had worked for this company for several years and was familiar with some legacy technology we had and had friends and co-workers who had knowledge of the current state of the systems. Over time, I heard about this flaw or that through comments such as, "can you believe they haven't closed this yet?" or "look what I just found!" Any one vulnerability can be a substantial risk, or it may be a complete waste of time to fix. A string of vulnerabilities, including web sites and source-code servers is worthy of attention. My suspicion is that the IT staff knew about many or all of the vulnerabilities, but not the ultimate risk exposed by those vulnerabilities. At best guess, based on information I had gleaned on my own and from others, my company had:

1. Passwords in web page .asp files. (visible from View-Source in a web browser)
2. Names of database servers in .asp files. (visible from View-Source in a web browser)
3. No hardware firewall, just a simple NAT solution
4. Dual-homed web servers, one NIC exposed to the Internet via NAT, one to the intranet.
5. Open connectivity between the web servers and our source code file server
6. A very weak administrator password on the source server.

With the exception of the source server, to which I was allowed access, I did not test these vulnerabilities.

[2] Sterling, Bruce Part 3.1 Introduction

During – Getting the Right Kind of Attention

I was well aware of the case of the well-meaning or "Good Samaritan" hackers. Obviously, in the case of a malevolent attack (for example, the case of a disgruntled employee at eEye Security[i]), the attacker should be prosecuted under the best available of the still-evolving hacker laws. By breaching systems, hackers violate federal and often local laws. But what consideration should they get if they report the hole and offer assistance on how to close the holes they exploited?

There are many hackers and groups who insist they hack with their targets' best interests at heart. For example, The Dynamic Duo professes to be assisting in national security by pointing out flaws. However, they point out the flaws by defacing web sites and posting sensitive information to the Internet. It's pretty clear that their claim of benignancy is an attention-grabbing ploy for the hacking community. "We are two individuals who risk our future and our lives to help the Nation in such a vulnerable time," the Duo wrote. "Somebody has to do it, if we don't, a terrorist might."[3]

Take the famous case of Adrian Lamo, for another example. Lamo has a history of hacking public websites and corporate intranets, but because he follows up by working with the company he hacked to help close the holes, he has been saved from prosecution so far[ii] (though his fate with the New York Times is still undecided). There is a wonderfully lively debate surrounding this issue[iii], but ultimately what matters to any individual is how the hacked system owners will respond to any specific incident.

In 1993, Randall Schwartz, usurped security on computers at his employer, Intel, to make his work for Intel more efficient. Intel saw things very differently and prosecuted to conviction three breaches of its systems (see State of Oregon v. Randal Schwartz[iv]). I have also heard anecdotally about other cases of employees with good intentions getting fired or prosecuted because they hacked a corporate system with the intent of illustrating security vulnerabilities. After all, if management doesn't believe that a hole is exploitable, what better way to prove it than to exploit the hole and show management the potential damage?

The way to do this is the way the General Account Office (GAO) does it. This example is more in the vein of social engineering. The General Accounting Office has a "Get Out Of Jail Free" (GOOJF) card. In March of 2002, investigators from the GAO were able to breach several federal buildings in Atlanta. These investigators not only do not face indictment for their published and admitted unlawful entry into FBI buildings (a federal offense), but they will probably get a raise. One would think that this sort of vulnerability assessment would prove Adrian Lamo's argument to management, until they read

> "[The NBC News correspondent] reported that same GAO unit successfully penetrated 19 of the government's most secure buildings in Washington two years ago, including the headquarters of the FBI and the Justice Department. A copy of

[3] Poulsen, Kevin, "FAA Confirms Hack Attack"

the GAO report on that investigation was recovered recently from a cave in Afghanistan."[4]

Merely discovering and reporting flaws does not lead to increased security, and may lead to higher security risks. And so the debate about Good Samaritan Hacking continues.

Alternative methods

I try to be a good employee, work for the advancement of the company and my stock, drive people and systems to be bigger and better, and of course, beat the competition. So how could I report these vulnerabilities without actually hacking into my company's computer systems and thus endanger my career both at this company and at any company to follow? I do not have a GOOJF card.

Everyone knows that it is important to secure computers and networks. Everyone knows there are hackers "out there". What people don't take time to assess are questions like "What is the likelihood I would get attacked?", and "What could happen if I were successfully breached?" This is assessing vulnerability and risk. Only after answering these questions can anyone realistically answer the question "What do *I* need to do to stop it?" What is enough expense? What is too much for the potential loss? What specific steps do I have to take?

The most important step to getting management to intelligently approve resources for securing systems is to make them answer the first two questions. Given that, management will let the IT and security people answer the rest. Not being able to get management's attention to answer them, I had to answer them myself:

Question: What is the likelihood my company would get attacked?
Answer: The web page content problem was actually reported to us by a job applicant. There is just no trouble at all in clicking View – Source and perusing the HTML. In addition, my company sold security software, so we *should* be targets of hackers who want to build their own reputations or damage ours as in the case of eEye Security.

Question: What could happen if I were successfully breached?
Answer: According to the vulnerabilities I had uncovered, and knowing that there are more out there that I don't know about, it seemed feasible that someone could access our source server. Between the lost intellectual property, which would probably have been posted to some web site, and the 100% certain bad press and thereby loss of software sales, it seemed like a huge risk.

Risk management is a standard component of management training, but computer risk management is not. Real education in technical computer security is finally starting to take off, after being a cult science for 15 or 25 years, depending on how you count it. Computer Security for management is still in its infancy. SANS training can only touch on full risk assessment while sticking to technical security.

[4] MSNBC "Federal Building Fail Security Test", AP "Fed Buildings Fail Security Test"

Management may not understand the technology, but *management knows publicity* and an email from SANS Newsbytes gave me an idea. Obviously, if management does not have a handle on security, then they do not have PGP to check the newsletter's digital signature. I modified the SANS email so that my company was highlighted as the third article, and I described a breach so realistic and damaging that it got exactly the sort of attention I was after. I sent this email to two vice presidents with whom I had a prior relationship, and two product managers who had an interest in seeing our systems secured. In retrospect, even a move like this could have hurt my career, since management does not want to be bothered fighting fires that don't exist, such as a publicity nightmare I manufactured. But certainly this was better and less intrusive than actually hacking into the systems. The relevant part of the email is attached as Appendix A.
Some example responses I got were:
From VP#1: "God did you scare me – I thought it was real. I sent it on to our new CIO also."
From Product Manager #1: "A truly excellent spoof."
From someone on the Bcc line with an interest in security: "Truly a work of art - hopefully someone listens and does something now."
VP#1 forwarded it to the new CIO and VP#2 sent it to the CEO inside of about 10 minutes of my sending it to them.

In an ideal world, merely sending an email to the people responsible for security, saying "you have this vulnerability, and I detect these risks" should give them and their managers heart attacks, but sadly this is not the case.

After – Realizing That it Did Not Burn

As it turns out, the chain of events that I created was not entirely realistic. By not actually exercising the exploits, I could not prove that they were truly sequential, or that all the holes were still open at the time of my sending the email. I traded perfect accuracy in exchange for job security.

One of the product managers forwarded to me the response from the IT director. He addressed a case where the hole I identified was old and had been closed. Some were not going to be fixed because the servers were going to be moving off-site (but my response to that is that these vulnerabilities had existed for almost two years and should have been fixed long before the move had yet been planned). Two (the web page contents issues) were in progress when I wrote the email. The remainder, including the weak password issue, were fixed within days of this email, but had not been in plan to be addressed until I sent it. I can only hope they used a strong password, but the important thing is that I, along with a couple hundred other people, no longer know what the password is. All the holes were closed within two weeks.

I am quite certain that the IT people responsible for security were very unhappy with me, since this email started quite a fire underneath them and created extra work. My defense, at risk of sounding like Adrian Lamo, who I do not admire, is that they were aware of

most of these vulnerabilities, had been warned or asked about them on several occasions and moved very slowly to address them.

This by itself is not a scalable method. Once managers hear that spoofed news articles or their variants are being used by well-meaning internal corporate hackers, they may either outlaw the disinformation that it represents (their employees are being dishonest), or they may just ignore it since it is a known "exploit" with no real impact. The point is that white-hat hackers without GOOJF cards must find alternate means for exhibiting vulnerabilities and risks to IT and management. It is important to "make it real":

- Keep examples realistic and based on the actual systems in place, rather than worst-case scenarios for what could happen to anyone connected to the internet.
- Show the risks without blowing them out of proportion.
- Be as concise as possible. Any hotly contested issue like this can get out of hand in debate. Make a point and be done, as Case Two presents:

Case Two

Presented in Case Two is my adventure of beating my head against a wall with the people responsible for networking and the people responsible for security at another company. After all, who cares about integrity of instant messages? In the following scenario, all company names and Instant Messaging aliases have been changed to… you know the rest.

Before – How Did You Get My Number?

Making it real does not always require sensationalism. In January through March of 2002 I was getting misdirected Yahoo! Messenger! (Y!M!) instant messages. It required no action on my part, so I couldn't be accused of hacking conversations. All I had to do was log into Y!M! and wait. Sometimes it would go days or weeks between problems. Then, eventually, I would start to get messages from people not on my buddy list. The most interesting part of these messages was that they were clearly not invitations to talk (like most people, I limit my conversations to people I know and do not invite conversations with "new friends"). These were people in the middle of a conversation with someone other than me. Worst of all, there was no detection of misdirection other than the fact that the intended recipient didn't get the messages and I did. There was the "sender", whose messages were arriving on my desktop, and the "intended recipient" who was supposed to be getting them and was not.

During – Cold Calling

Tracking this down represented an interesting challenge. Because of the way the Y!M! client window would pop up, I could see who was sending the message as well as the intended recipient. If I attempted to respond the Y!M! servers would recognize that the session was invalid and would require me to log out and log back in.

At first, I tried contacting the sender to let him or her know that his/her messages were not getting through. While this was an attempt at being a good net-citizen, it elicited great distrust. How would *anyone* respond if an unknown instant messenger user tried to entice them into a conversation with the introduction line "I am getting your messages to so-and-so."? My conversations went as would be expected, with little headway and a lot of suspicion directed at me. Ultimately, there was not really any client configuration that could cause their messages to get misdirected, so this quickly proved itself to be a dead-end anyway.

Next, I tried contacting the intended recipient. I would add them to my Y!M! buddy list with an introductory message just as gentle and unassuming as I could. Something like "I am getting messages from so-and-so for you. Please add me to your list so we can talk and troubleshoot."

Eventually this worked. At this point, it had been a problem for about two months.
The first good bite I got from an intended recipient resulted in a conversation that went something like this:

Me: You don't know me, but I'm getting messages meant for you from DayTrader32
Me: Like this (paste)
DayTrader32: yeah, that's what i was thinking
DayTrader32: r u going with them?
DayTrader32: im really bored
FunkyDesign: how are u doing that? (recognizing responses to FD's messages)
Me: I don't know. It just pops up. I was hoping you could work with me a little bit to troubleshoot.
FunkyDesign: That's so weird
Me: I know.
Me: Where is DayTrader
FunkyDesign: she's in Hawaii
Me: Hm. I don't suppose you are anywhere in the Gulf Coast?
FunkyDesign: yeah.
FunkyDesign: that's so scary
Me: I know. (at this point I started to suspect network misrouting)
Me: You're in Florida, aren't you?
FunkyDesign: yes, howd you know?
Me: You wouldn't happen to be on the corporate network at Liposuction, Inc. would you?
Me: I am. I'm in building G.
FunkyDesign: yes i am. i'm on the Tourbus campus.
Me: Okay, I have an idea. I'll contact IT and see if they know anything about this
FunkyDesign: okay

I never got FunkyDesign's name or email address inside Liposuction, Inc. I opened a ticket with our IT department, but they didn't really have any understanding of why this would be happening. They asked me to collect some information if it happened again.

The next time it happened, I was able to write to the intended recipient with something a little more meaningful, like "Hi, I'm getting messages meant for you from TheLastStop21 and I'm working with Liposuction's IT group to figure out why. Please add me so I can collect some info." By the fourth and fifth case, I was getting phone extensions, talking to people directly, getting IP addresses from them for troubleshooting (which gave me some interesting ideas for social engineering, but that's another story), and copying them on my correspondence with the networking team.

There is a corporate policy that no sensitive or proprietary information is allowed over internet instant messaging protocols because a) they are sniff-able and b) they are archived on some other company's server, representing a security breach. This is a good policy, and if followed reduces the risk of misdirected instant messages. However, there is still the issue of lost productivity, since these tools are used for work, and there is the more personal question of at least the perception of confidentiality in a conversation. People simply would not like it if the network allowed for inadvertent conversation sniffing. So I again asked myself the questions on vulnerability and risk:

Question: What is the likelihood it would happen?
Answer: 100%. It happens by itself.

Question: What could happen if I were successfully breached?
Answer: Not too much, financially. As long as employees are abiding by the policies, no sensitive information is going across these connections. However, there is a privacy concern and a perception of computers that should be maintained.

It was relatively low risk and therefore not fighting about, but it was a breach of privacy that was worth at least the effort of pointing it out to the appropriate people.

After – Fixing It, Then Fixing it Again

After a few rounds of troubleshooting and looking through our router logs, the IT department narrowed it down to overloaded stateful routers and the fact that Y!M! uses UDP which is connectionless. The response of the IT department was to tell me to change my Y!M! configuration to use the HTTP proxy rather than simply trusting the network to route internet traffic. There is a huge problem with this: I could just change it back, and anyone else could have it in the "wrong" configuration and never report it to IT. This is not acceptable because IT is *allowing misconfiguration* by putting the onus on the end-user to configure it right, without dictating any configuration policies. The best solution is to change the firewall configuration so that the wrong Y!M! client configuration *won't work*.

The person I was working with on the networking team wrote a letter to me and copied the security team at Liposuction, Inc. He explained that it was up to the security team to determine whether instant messaging, and in fact, which of all software was allowed on company machines. They also had authority over networking security. Deliberately or not, he made the email sound like I was introducing useless work for the security team

never a welcome thing. My response was to acknowledge that it was ultimately their call and I would not fight about it, but I had to explain why allowing misconfiguration was a problem (see Appendix B for the email conversation). Security responded to networking that this should be solved if possible. Ultimately, the networking team disabled caching from the Y!M! servers' IP addresses and this appears to have eliminated the problem regardless of my client configuration.

Conclusion

According to government posted data, the number of cracks perpetrated by malevolent employees roughly matches the number of cracks perpetrated by real hackers[v]. There is an argument in the security community regarding the relative percentages of attacks from external or internal sources. I would argue that this is miscalculated based on semantics. There will always be more port scans and probes from external sources simply because there are more people, primarily script kiddies, looking for vulnerabilities. On the other hand, insiders tend to have more knowledge of the systems, tend to not need brute-force tools such as port scans, and are therefore much more likely to execute highly surgical attacks on vulnerabilities discovered from sources other than software tools.

In any case, companies' awareness of internal hacking, for any goal, is on the rise. Employees, especially SANS students, may know too much about networking and system security for their own good. The common philosophy is that the best way to attract attention to system vulnerabilities is to exploit them and show what damage *could be done* without necessarily doing damage. Of course, in the case of The Dynamic Duo, there is even the argument that one should *do the damage* to fully draw attention to it. Obviously, I do not support this philosophy, but without it, what options do SANS students and other security-buffs have?

My argument is that we should work to come up with creative methods for "making it real" to management, when it comes to security vulnerabilities. This requires risk assessment on the part of the Good Samaritan, especially if the company is not doing risk assessments. The Good Samaritan will quickly lose credibility if he or she points out vulnerabilities with no real risk ("look, I can crash the print server with a ping-of-death" "Yes, but our company is paperless by policy"). Generally, it is easier to find vulnerabilities by having contextual information, such as what the old domain administrator password was before the company grew to its current size, what sort of networking expertise is available for the person installing the firewall, and so on. This information is available to an employee without any hacking. However, it is worthwhile to gather a little more information ("what is on that server with the weak password?" "is that firewall connected to the internet or DMZ, or is it just between corporate branches?") before waving red flags to senior management.

But once you have that information and have evidence that the exposure is substantial, make it real by explaining the financial loss, the bad publicity, or using some means other than exploiting the vulnerability and hopefully the laws against Adrian Lamo's activities can be enforced with less debate.

Appendix A

-----Original Message-----
From: Michael Eisenstein
Sent: Friday, April 13, 2001 11:23 AM
To: Vice President 1; Vice President 2
Cc: Product Manager 1; Product Manager 2
Subject: FW: SANS Newsbites Vol. 3 Num. 15

Check out the third article. You'll have to scroll down to get to the text.
-Mike

-----Original Message-----
From: sans@sans.org [mailto:sans@sans.org]
Sent: Wednesday, April 11, 2001 7:21 PM
To: Mike Eisenstein
Subject: SANS Newsbites Vol. 3 Num. 15

****
To: Mike Eisenstein
From: Alan for the SANS NewsBites service
Re: April 11 SANS NewsBites

****

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

****

SANS NEWSBITES

The SANS Weekly Security News Overview

Volume 3, Number 15 April 11, 2001

Editorial Team:
Kathy Bradford, Crispin Cowan, Roland Grefer, Bill Murray,
Stephen Northcutt, Alan Paller, Howard Schmidt, Eugene Schultz

****

TOP OF THE NEWS
10 April 2001 Alcatel DSL Models found vulnerable
6 April 2001 Outlook 2002 Will Restrict Attachments
5 April 2001 Software Vendor SoftSekyur Web Site Hacked, Source Code Stolen
5 April 2001 GAO Says DOE Doesn't Adequately Clear Old Machines
3 April 2001 Wireless LAN Protocol Vulnerabilities
2 April 2001 Web Host Database Stolen

THE REST OF THE NEWS
6 April 2001 Security Projects Likely to Survive Budget Cuts
5 April 2001 FedCIRC Outsources Operations

5 April 2001 Turbo Tax Glitch May Necessitate Password Changes
5 April 2001 Two Indicted in Cisco Stock Theft
5 April 2001 New NIPC Director Accentuates Preventive Security
              qMeasures
5 April 2001 CA Democrat Site Security Hole
5 April 2001 Yahoo and eBay Log-Ins Not Always Secure
5 April 2001 Welsh Cracker Says He Used Gates' Credit Card
4 April 2001 IT Should Work With Legal Department
2 & 3 April 2001 eBay Privacy Policy Modified
2 April 2001 Industry Says Virus Challenge Irresponsible
2 April 2001 Cloaked Code
2 April 2001 Security Disclosure Could Raise Confidence in Internet

UPCOMING TRAINING AND CERTIFICATION CONFERENCES
   SANS 2001, May 13-20, Baltimore: http://www.sans.org/SANS2001.htm
   Orlando, April 18-20: http://www.sans.org/springbreak.htm
     --- Orlando is SANS' largest regional featuring the most popular
         tracks from SANS 2001
   London, June 20-23: http://www.sans.org/london2001/index.htm
   Raleigh, April 10-12:
          http://www.sans.org/trianglepark/trianglepark.htm
Plus ten more posted at http://www.sans.org

********* Sponsored by VeriSign - The Internet Trust Company *********

Secure all your Web servers now - with a proven 5-part strategy. The
FREE Server Security Guide shows you how:

    DEPLOY THE LATEST ENCRYPTION and authentication techniques

DELIVER TRANSPARENT PROTECTION with the strongest security without
disrupting users. And more.

Get your FREE Guide now: http://www.verisign.com/cgi-
bin/go.cgi?a=n061207810014000

****

TOP OF THE NEWS

 --10 April 2001 Alcatel DSL Models found vulnerable
Tsutomu Shimomura, a senior fellow at the San Diego Supercomputing
Center, discovered numerous flaws in a popular modem supplied by
Pacific Bell, Ameritech, Bell Atlantic and others to DSL customers.
http://www.uniontrib.com/news/business/20010410-9999 1b10dsl.html

 --6 April 2001 Outlook 2002 Will Restrict Attachments
In an effort to protect users from viruses, Outlook 2002 will reject
more than 30 types of file attachments, including .exe, .bat, and .vbs
files, CD images and screen-savers. The new restrictions will make it
more difficult for people to share information as the feature is very
difficult to disable. Security expert Richard Smith supports
Microsoft's endeavor and suggests people compress files they wish to
send to others; other experts believe Microsoft should fix its

essential security problems instead of treating the symptoms.
http://news.cnet.com/news/0-1003-200-5529034.html?tag=prntfr

--5 April 2001 Security Vendor SoftSekyur Web Site Hacked, Source Code Stolen
Hackers gained root-privilege control of numerous servers at SoftSekyur Corporation in April. Hacker group LudXe immediately claimed responsibility when the hack was first reported by the Seattle Times (http://seattletimes.com) on April 4th. LudXe typically attacks security software vendor websites like RealSecure (http://www.realsecure.com) and McAfee (http://www.mcafee.com) as a matter of principle, according to the Times article.
SANS has monitored LudXe's activities for about 27 months, since a quiet, but very damaging attack on EDS in late 1998. LudXe founding member Ste1%n wrote to SANS and told us that cracking the SoftSekyur web site had been "ridiculously easy", so they proceeded to delve further into the SoftSekyur intranet. "We wanted to see how far we could get," said Ste1%n in his email to SANS. "Once we took control of the web server, sniffing network packets was easy, so we got free passwords that SoftSekyur employees were passing in clear text to POP3. Lophtcrack picked up the administrator password on their source code server in about 15 seconds and the download frenzy was on!" wrote Ste1%n. "This crack was by far the most trivial to do, relative to the security sites we have hacked in the past."
SoftSekyur declined to comment on how long the download went on before it was discovered or how it was discovered. "We are still investigating the depth and duration of the penetration," said Fred Flintstone (I used the real IT director's name here –Mike), director of IT at SoftSekyur. SANS is particularly concerned about the growing duration of this internal investigation, since SoftSekyur markets and sells eHarden, a tool for hardening Windows systems. Now at this point should SoftSekyur's statement to the public be that we weren't running eHarden on our systems, or that eHarden didn't stop these very simple cracks? Also, every one of the holes mentioned in this **bogus** article is real and this chain of events is realistic.

I am talking less about network security and more about credibility in the space into which we have been selling eHarden for the last seven and a half years.

Consider:

- We've received emails from outsiders that indicate that they have penetrated our web server and read some relatively sensitive information from the web pages.
    - Deductions: We have the attention of hackers, and it's possible we could already have been hacked and we'd never know it.

- Our web servers are dual-homed to the Internet and the intranet. If someone takes over a web server, it would be very easy to proceed inward. Security best-practices state that it should be assumed that web servers _will_ get compromised, even inside a DMZ.

- We have no real firewall. Security best-practices dictate that there should be a firewall both between the Internet and the web servers _and_ between the web servers and the intranet.

- We haven't run eHarden on our internal systems, web server, file server, source code server, etc.
  - Deductions: we aren't using and testing our own software and we aren't deriving the value/benefit we are claiming others would derive by *paying* for this software.

- The administrator password on SRCSVR is one known to every employee and former employee of SoftSekyur employed prior to about 24 months ago. In addition, this password is a very weak one, which Lophtcrack did pick up in about the time described in the article. SRCSVR stores ALL of our source code.
  - Deductions: you can make your own.

- Email is available over POP3. I personally derive a massive benefit from this, since I have to check my SoftSekyur mail from a customer's intranet, and MAPI is not an option. Our POP3 is unsecured, though. Adding SSL to POP3 is trivial, but not in place. My password goes out over the internet in clear text every 15 minutes like clockwork as long as my Outlook client is open. This goes for Outlook Web Access as well.

Some suggested fixes, without engineering an entire solution:

1. Get keys for digital signatures and public key encryption from Verisign. These are cheap and useful. We should also be signing our software, but that's another story. Windows XP is going to be less friendly to unsigned software when it ships later this year.
2. Get real firewalls. They make a big difference, and when you consider the cost of a hack like the one above (source code loss, bad PR), they are cheap.
3. Put SSL on POP3. This is a matter of getting a key and checking a checkbox (and having people like me make minor changes to client configurations).
4. Run eHarden on production systems.

-Mike

Greetz (and thanks) to the following for their information/advice contributing to this dramatization:
(here I listed people who had helped me learn of the various vulnerabilities and who had toiled fruitlessly in fighting for better security on our systems. I've pulled them out for sanitization -Mike).

This message was sent internally at SoftSekyur by POP3.

--5 April 2001 GAO Says DOE Doesn't Adequately Clear Old Machines A General Accounting Office (GAO) report reveals that the Department of Energy (DOE) has no policies for managing used computers and that some retired machines still contain readable data. DOE regulations require that all information be cleared from computers before they are transferred. The GAO recommends that DOE develop and implement

procedures for clearing hard drives and that they obtain independent verification that machines have been properly cleared.
http://www.fcw.com/fcw/articles/2001/0402/web-doe-04-05-01.asp

--3 April 2001 Wireless LAN Protocol Vulnerabilities
A research team from the University of Maryland has identified three new wireless LAN security problems, all dealing with access control and authorization requests. One allows an eavesdropper to sniff the
<Remainder of SANS news email snipped>

Appendix B

-----Original Message-----
From: Michael Eisenstein
Sent: Thursday, April 11, 2002 2:07 PM
To: Networking Team
Cc: Information Security Team
Subject: RE: Y!M! sessions crossing

I agree that it's the security team's call, both to determine what software is allowed inside on the corporate network as well as how the network security is configured. Certainly having clear-text traffic routed through a third-party server is something they should consider and make a command decision on.

On the other hand, to blame Yahoo for my particular problem as a "security hole" is a bit of burying our heads in the sand. What we have here is (routing solution deleted) misrouting traffic. It could be that (routing solution deleted) is routing messages to machines without a Yahoo IM client installed, in which case the user never sees it. In my case, because I have a client, it picks up the "new conversation" and shows it to me. When this happens, the intended recipient does not get the messages. Perhaps if we could prove that somehow my client "subscribes" to the network or (routing solution deleted) in such a way that it could intercept traffic, that would be some bad points against Yahoo software. If this is not what is happening, though, then the points are against (routing solution deleted), and I don't think our corporate security concerns would abide by this.

Configuring (routing solution deleted) so that the Yahoo client won't work unless it's configured to use an HTTP proxy is a reasonable workaround. Leaving (routing solution deleted) so that the client works either way exposes this hole (provided that is proven by the experiment we are currently running). Ultimately, if it could be proven that it is an (routing solution deleted) code problem, it should be reported to the vendor, just as proving that it's a Yahoo problem should be reported to Yahoo.

These are my philosophies on product and security and I feel I would be amiss if I didn't communicate them. With that done, the rest is up to you guys. Thank you for humoring me.

-Mike

-----Original Message-----
From: Network Security Team
Sent: Thursday, April 11, 2002 1:56 PM
To: Michael Eisenstein
Cc: Information Security Team
Subject: RE: Yahoo IM sessions crossing

I'll throw it to the security guys to consider. Looks like Yahoo MAY have some software that could be a security problem.

Maybe Security might want to ban its use. We believe that it is possible to reconfigure (routing solution deleted) to open port 5050 as a work around. Opening this port would require an engineering change and security would have to approve it. I'm wondering if they would go for it? Moving clear text communications between our employees out through another corporation's server? That's now our call.

Thank you,

Networking Team

Appendix C – Sources

Endnotes:

[i] Kelly, Lisa "Chief Hacking Officer attacked on the web", 12/15/00 URL: http://www.vnunet.com/News/1115570 (4/30/02)

[ii] Poulsen, Kevin, "Panel Debates Hacker Amnesty", 4/25/02, URL: http://thehacktivist.com/modules.php?op=modload&name=News&file=article&sid=355 (4/30/02)

Lemos, Robert, "Hacker helps Excite@Home toughen defenses", 5/29/01 URL: http://news.com.com/2100-1001-261728.html?legacy=cnet&tag=mn_hd (4/30/02)

Hulme, George V., "Hacker Points Out WorldCom Network Flaw", 12/6/01, URL: http://www.informationweek.com/story/IWK20011206S0016 (4/30/02)

Reuters, "New York Times internal Web site hacked", 2/28/02, URL: http://www.ciol.com/content/news/repts/102022804.asp (4/30/02)

[iii] Forno, Richard, "Beware the Kindness of Strangers: The Case Against Good Samaritan Hackers", 3/28/02 URL: http://online.securityfocus.com/columnists/70 (4/30/02)
also see Discussion links at end of page

[iv] State of Oregon V. Randall Schwartz, 1993-1995. URL: http://www.lightlink.com/spacenka/fors/ (4/30/02)

[v] Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) URL: http://www.cybercrime.gov/cccases.html (4/30/02)

Bibliography

Lisman, Jarrad, "Adminstrator Complacency: A Real Threat to Network Security", 2/12/02 URL: http://www.giac.org/practical/Jarrad_Lisman_GSEC.doc (4/30/02)

Sterling, Bruce, "Law and Order" Hacker Crackdown 1/1/1994, URL: http://www.lysator.liu.se/etexts/hacker/lorder1.html (4/30/02)

Poulsen, Kevin, "FAA Confirms Hack Attack", 4/25/02, URL: http://online.securityfocus.com/news/378 (4/30/02)

MSNBC, NBC, AP "Federal Buildings Fail Security Test" (4/29/02)
URL: http://www.msnbc.com/news/745303.asp?0dm=C14QN
URL:
http://story.news.yahoo.com/news?tmpl=story&cid=514&ncid=514&e=9&u=/ap/20020430/ap_on_go_ca_st_pe/security_breaches_7 (4/30/02)
(Two links included in case one expires)