Global Information Assurance Certification Paper

Hotmail, why free email might not be such a hot idea.

Written by Michael Barrett
SANS Security Essentials Version 1.2f
This practical is written to satisfy the Level1 GIAC Security Essentials Certification.

Microsoft is under scrutiny for problems they have in all areas of computers. I chose to focus on Hotmail which is a single aspect of the Microsoft empire and probably the most widely recognized component. I believe due to the nature of email being accessed by almost all users of the Internet, security problems with these systems impact the biggest group of people who have on average the least amount of security savvy on the Net.

Millions of people, including me, use free email services on the web, probably the most popular is Hotmail. Microsoft purchased the Hotmail system in 1997 for $400 Million dollars, at the time with a subscriber list of around 9 Million accounts. Since Microsoft has taken over the systems they have seen tremendous growth, to date Microsoft claims 110 Million subscribers. As the system grew, Microsoft began migrating functions off the primarily Unix and FreeBSD based systems to Windows platforms to “do a better job” handling all the new traffic on the site. This is where some believe Microsoft’s troubles really began. Many people are of the opinion that the Windows operating system is not as secure as other operating systems. I believe that the problem lies not with the operating system but how it is configured and maintained. The Windows platform can be made secure by providing the proper maintenance such as patches, hot fixes and upgrades necessary to repair problems all programs have, regardless of platform.

Many people have a bone to pick with Microsoft and what a better way of getting back at them than causing problems with a highly visible site like Hotmail?

As early as 1998 people started making trouble for Hotmail. A Canadian Web developer (Tom Cervanka) reported an insecurity in Hotmail that would allow a cracker access to a user’s password by spoofing the user into re-entering their username and password into a crafted MacroMedia Shockwave attachment that appeared to be the normal login screen presented by Hotmail. If the user re-entered his credentials they would be emailed directly to the cracker. This type of trick follows similar exploits using JavaScript to fool the user into re-entering their credentials. Microsoft made attempts to protect against these types of attacks but did not go far enough, because browsers default security configuration are typically wide open and can leave them susceptible to these attacks. Browser security settings are one of the key factors in a user’s ability to guard against such an attack. If more people would use the correct settings to (at the least prompt) the user when other types of code try to run on their machines, i.e. JavaScript or ActiveX, less of these types of attacks would be successful.

Cookies are for more than just eating.

In March 1999, Microsoft attempts to plug security holes in the Hotmail systems by mandating the use of Cookies. Cookies are a general mechanism which server side connections, such as CGI scripts, can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of Web-based client/server applications as opposed to using the IP address of the user. According to a Chicago

software engineer, malicious users can dig URL's out of users' history files and swap out information to gain access to other user accounts as long as they are logged onto the system. Privacy advocates criticize the Cookie concept as it stores information about users that could fall into the wrong hands. Users have many options for the use of cookies and all too often fail to utilize the most secure method. Cookies can be viewed as fingerprints left behind all over the Internet and users need to make themselves aware of what they could be leaving behind. In the security field, paranoia is your friend. If you think something you are doing on the Net could be turned against you, odds are someone has or will find a way to exploit it. I would like to stress again that the users as well as the manufacturers, are critical in the security role of the Web.

Microsoft patches problem?? Account still available without password.

In late August 1999 Microsoft claimed to have patched their systems problems that allowed people to access accounts without a password, but testing proves otherwise. After Microsoft was alerted that two of their servers (one in the UK and another in Sweden) were allowing access without a password, they brought the sites down and repaired the problem. According to Microsoft there was a second security problem, which was blamed on hackers. Apparently a programmer published an application that stored login ID and an old login script on the affected servers. Some analysts point the problem at the recent updates done on Hotmail servers as part of the Passport launch. Passport is a Microsoft initiative aimed at bringing all user ID's and passwords together making it easier to access the Web and purchase goods and services. Many times application problems like this can be directly linked to a failure to follow documented policies, or in the worst case no policy at all. A very large percentage of security issues stem from known vulnerabilities and flaws. Very often these problems are overlooked or put aside due to the tremendous pressures on IT staffs to keep production servers online and on schedule.

Audit of Hotmail systems not to be made private.

In late 1999, Microsoft commissioned an outside audit of the Hotmail system to verify the fixes put in place after a vulnerability was discovered that allowed anyone access to users accounts by simply knowing their email address. Microsoft and the Web privacy program, Truste, claim this is a step towards improving privacy. Junkbusters, a privacy-protection group, sent a request to Microsoft and the Federal Trade Commission for the details of the report. Microsoft however refused to make public the findings of the audit claiming they were prohibited by the American Institute of Certified Public Accountants (AICPA) from revealing the details of the report. The Truste seal is intended to protect information on the Web and investigate complaints, which is what happened in the Microsoft cause. Since Truste only suggested the audit, it seems Microsoft slipped through a loophole, which allowed the investigation to remain private. "The big difference to keep in mind here is that we never got to the stage where we mandated Microsoft to do the audit. If that had been the case, then we might be in a different situation. We hope it can be made public," said Truste spokesman David Steer. The privacy advocates insisted that Microsoft and the accounting firms disclose the details of their finding and it's opinion no later that a week after its delivery to Hotmail. I happen to believe that it is not appropriate to disclose the outcome of the audit, since the audit was voluntary and made to verify the corrective actions Microsoft performed to repair issues they have already acknowledged. Companies should feel safe in knowing that audits done on their systems are for their eyes only and used to protect themselves. I believe that full disclosure gives too much information to those who would have otherwise not had such easy access to the information.

Merry Christmas Microsoft, Linux programmer gives the gift of registration to Passport.com.

In an embarrassing chain of events around Christmas 1999, Microsoft failed to pay the $35.00 registration fee for the Passport.com domain name. This minor oversight on Microsoft's part resulted in an outage of the Hotmail system. A good Samaritan from the Linux community used his own credit card to pay the fee and Hotmail was back on line. Hotmail staff estimated that half of the 52 million users were affected by the outage. Passport.com is the authentication mechanism for Hotmail users which verifies the login and password attempts. Users who had already logged in when the domain expired were not affected, as were some users who were able to authenticate through another system through a process known as caching. While this problem really didn't pose a true security risk to the Hotmail system, it speaks to the enormous amount of work it takes to run such a system and how something as small as paying a bill can have dramatic effects on such a system.

Email like it's 2099.

New Year's Day 2000, Microsoft was bitten by the Y2K bug in the Hotmail system. Users who posted messages before November 1999 display a creation date of 2099. Microsoft took its time fixing the bug, as it was only cosmetic and chose to focus its resources on other more dangerous problems with Hotmail. Microsoft was fortunate that the problem they encountered was so minor. If a Y2K bug were to have been overlooked in other parts of the systems this could have had a much more dramatic effect on the system.

Bulgarian programmer reports yet another security flaw in Hotmail.

According to Georgi Guniski a Bulgarian programmer (who is interestingly referred to as a hacker in another article), a flaw in the filtering of JavaScript would allow users to be tricked into entering their credential to a fake login screen. Using JavaScript commands through an HTML tag in an email message could circumnavigate Microsoft's attempts to filter malicious code, leaving their users susceptible to trick attacks. Guninski demonstrated through the use of obscure and defunct images tags that he could circumvent filtering methods put in place. Guninski proved that the tags LOWSRC and DYNSRC, which were originally intended to increase the usability of browsers, could be used to attack a user due to the nature of the tags. Issues like this must leave people wondering how many more "hidden" features/flaws can be out there waiting to be discovered. Microsoft claimed to have no evidence that suggested the flaw affected any Hotmail users. I believe this problem demonstrates how far reaching security problems can be. It is hard enough to protect your systems from well-known methods of attacks, but when people start using defunct or hidden features it makes this task even more complicated.

Hackers Unite claim to discover "backdoor" in Hotmail systems.

A previously unknown group of hackers reported in late August of 1999 that they had discovered a hole in Hotmail security. Through the use of several Web addresses a user's login name was the only input required to access other user accounts. Access to these accounts varied from viewing message titles to full access including forwarding and sending emails assuming the identity of the other user. Microsoft denied the existence of a "backdoor" in Hotmail systems, and called the problem an unknown security issue. After learning of the problem at 2 a.m. PST Microsoft

engineers were able to generate the initial fix by 10 a.m. and fix a variant of the same problem by noon. They then began the difficult task of propagating the fix to all the Hotmail servers. Chances are this problem may have been known to Hotmail staff before the incident occurred, or not, and an independent security audit may have uncovered the flaw before hackers where able to exploit it. Often companies fail to get an outside or impartial view of their security until it's too late. Periodic internal and external audits can only lead to a more stable and secure system.

Please pass the Cookies.

In May of 2000, Microsoft patched a security hole, which allowed intruders to break into a user's email account by sending an unwary user an attachment of an HTML file. When the targeted user views the HTML file, their Cookies were intercepted and sent to a hostile site. Once the intruded has acquired the users Cookies they can be used to access the users account. An "anti-censorship" site offered the HTML file for download with instructions for usage. The site also offered suggestions for Microsoft and users to more safely use email by filtering JavaScript attachments, and also prompting users about the unsafe nature of some types of documents. Microsoft quickly repaired the problem and the exploit was shortly outdated. The problem here falls on the shoulders of the users and Microsoft. Far too many users use the Internet in unsafe ways and fail to understand their role in security.

How safe are your email attachments?

Late July 2001 left Hotmail users susceptible to the Sir Cam worm. Hotmail users benefit from the added feature of McAfee virus scanning on all attachments sent through the system. Unfortunately this can lead to a false sense of security on the part of some less educated (or trusting) users. Microsoft was left open to the Sir Cam worm due to the outdated nature of the virus definition files. At the time the bug was known for nine days and Microsoft had not yet applied the update to protect its users. Users should be aware that everyone shares the responsibility of security and they should not rely on one source to check for malicious applications. A virus scanner on all user machines is necessary. Above all, unsafe behavior is responsible for many of the problems in today's Internet community. If users would invoke more common sense when using their computers many of the problems with viruses we see today would not be as bad. All users should use the simple rules when handling email: Do I know this person? Am I sure this email came from the person? Was I expecting an email/attachment from this person? Did I scan the attachment before opening? These steps often elude people that are either too lazy or too careless to exercise their own common sense.

Root-Core publishes a new Hotmail flaw.

In August of 2001, the hacker and security site, Root-Core, publicized a vulnerability, which allowed others to view private emails. Microsoft said the problem existed, but it was a mathematical improbability to utilize. The exploit involves customizing a URL based off an existing URL obtained by legitimate access to Hotmail. Hotmail uses a "predictable" sequence in their mail numbering system, which is based on the UNIX time stamp and an additional two-digit number. A hacker could replace these numbers in a malformed URL to gain access to other's mail. Microsoft points out that it may take thousands or hundreds of thousands of guesses in order to trick the system, which may be interrupted by Hotmail's security systems. Root-Core used computers to automate

the task of guessing numbers and posted the tool on their web site. The vulnerability brought unwelcome attention to Microsoft's increasing reliance on the Passport authentication systems and the integration into their newest release Windows XP. On a side note the vulnerability also points out that Microsoft has not yet weaned themselves off of UNIX systems completely, leaving some speculation over the migration of Hotmail from an open-source system to strictly Windows 2000 based environment.

Have hacks will travel.

Some hackers have even offered their services to gain access to user accounts. A hacker calling himself The Hunter offered a service on an Internet forum site to crack any Hotmail or Yahoo user account. The Hunter claims to have a system that will always work to discover user credentials. He sells his service for $50.00 and offers proof by sending an email from the victim's account to the person wanting the information.

I was also able to find programs intended to break the password by "brute force" the application could be purchased for $14.95 and claims to hack passwords for sites using HTML (like porn sites). It also claims to work on FTP, HTTP and POP3. The advertiser points out that the software is illegal to use on other and is intended for "reverse engineering" purposes. They also chose to list a disclaimer that states it could cause servers to crash and that the user was responsible for any damages.

While there will always be dishonest people in the world offering to do dishonest and illegal things the focus should be on how we use technology and how we can use it safely. Anyone using the Internet should be aware that the information they are sharing travels over many devices, all of which have the potential to be compromised. People should do all they can to protect themselves from prying eyes.

Some users complain they are treated like children.

Dave Miller has had quite a few problems with Hotmail since he started using it in 1995. His most frustrating problem is Microsoft treating him like a child, literally. Dave made a mistake when setting up an account for his daughter and accidentally configured his Passport to be a child's account by entering his daughter's birthday. He has made several attempts to rectify the problem but Microsoft support claims there is nothing they can do. Once he was made a child, his account cannot be changed to that of an adult's. No real explanation of why this could be was supplied, except to say that Dave should continue to use the process of giving himself permissions through another parent account. Although this problem seems minor, one must keep in mind that it relates to the Passport system Microsoft has put heavy faith into and uses as part of the Windows XP operating system and it's .NET initiative. If Microsoft is unable to rectify a simple problem such as this, how do they hope to handle the inevitable problems that will come up as they grow the use of the Passport system?

Closing thoughts and suggestions.

In my opinion there is no such thing as a 100% secure system, and there never will be. As long as

there are curious people out there we will continue to find flaws and quirks in computer systems. The best way to approach the Internet or for that matter any situation is to treat it as a threat and educate yourself sufficiently to protect yourself. Common sense is always the first and foremost way to protect yourself. Experts have been telling us for years and years, don't open emails, attachments, etc. from people we don't know or are not expecting things from. Use virus scanning software and update signature files regularly. Paranoia and fear are your friends. If something doesn't seem to make sense it probably doesn't. Erring on the side of caution rarely causes more problems than taking a chance on the unknown.

Information is readily available on manufacturers site and information sites all around the Internet. Most people who are victims are a result of outdated software or practices. If you are using the Internet in a corporate environment your company most likely has guidelines on safely using the Net and acceptable use of it. Read and follow these guidelines and you will most likely be in pretty good shape.

A few words on Microsoft and Hotmail. I have and will continue to use Hotmail and related applications provided by Microsoft. I do always keep one important thought in mind, which is to never write or chat anything you wouldn't want anyone else to see, because chances are the information could fall into the wrong hands. Hotmail is a convenient, easily accessible tool I have used all around the world. If used cautiously it's a great way to keep in touch. Users of Internet based email systems (or any mail system for that matter) must always keep in mind that the information they are sending could fall into the wrong hands. Encryption techniques are available for free or at low cost for those documents that need to be sent over the Net that must remain private.

Sources

CNN.com

http://www.cnn.com/TECH/computing/9908/30/hotmail.02/
http://www.cnn.com/TECH/computing/9908/30/hotmail.06/

c|net News.com

http://news.cnet.com/news/0-1004-200-332525.html
http://news.cnet.com/news/0-1005-200-120509.html
http://news.cnet.com/news/0-1005-200-1508169.html
http://news.cnet.com/news/0-1003-200-6941020.html

Infoworld

http://www.infoworld.com/articles/ic/xml/00/01/04/000104ichotmail.xml

INFOsec.com

http://www.info-sec.com/internet/00/internet_010600a_j.shtml

Netcape.com

http://home.netscape.com/newsref/std/cookie_spec.html

peacefire.org

http://www.peacefire.org/security/hmattach/

The Register

http://www.theregister.co.uk/content/56/20642.html

Salon.com

http://www.salon.com/tech/feature/2001/08/21/hotmail/print.html

Shop 4 Hackers

http://www.users.freenetname.co.uk/~sandradelgado/hotmail1.htm

Techweb.com

http://content.techweb.com/wire/story/TWB20010216S0024

Voy.com

http://www.voy.com/13609/298.html

Wired News

http://www.wired.com/news/technology/0,1282,14751,00.html
http://www.wired.com/news/technology/0,1282,21503,00.html

ZD Net

http://www.zdnet.com/zdnn/stories/news/0,4586,2323960,00.html

Last Updated: September 19th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event