GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

A Security Perspective of Microsoft Xbox

By James Anderson
GSEC Practical – Option 1 – Version 1.4b
06/04/2003

ABSTRACT

The Xbox is a popular Home Entertainment Console from Microsoft. The device's intended purposes are to play video games, and to playback Music .wav files and DVD movies. Consumers use the device mainly for these purposes, and with the addition the Xbox Live gaming service, they can now interact with other Xbox users over the public Internet. Due to the close nature of the Xbox components and the Personal Computer architecture, questions arise about whether this consumer product is subject to any known PC-related vulnerabilities. The purpose of this paper is to describe the facets of Xbox from an InfoSec perspective, publish results of GSEC-courseware security tools used against the Xbox, and make conclusions regarding Xbox security. This paper will find that the console in an un-modified form provides protection from malicious code and network observation. However, evidence is given that PC-type vulnerabilities are possible and the paper makes a call for further research and analysis on these aspects.

Xbox Architecture Overview

To begin the analysis of Xbox Security, one must ask what components make up the console. The Microsoft Home Division marketing team touts the hardware components as being the best among all game consoles. The unit is described as featuring an Intel 733Mhz CPU, nVIDIA GPU, Ethernet port, and internal hard drive. These components being very similar (if not the same) to standard PC components, beg the question of what software runs the Xbox? Microsoft does not publish this information publicly, but a quick search of the Internet shows that the Xbox runs a miniscule version of Windows 2000. This custom Windows O/S is stored in two parts, one part on the hard disk and one on the DVD-game discs. This would indicate that the O/S interactively loads O/S components as needed and provided by the game developers.

If the Xbox is running a custom, miniscule Windows 2000 created by Microsoft, what portions of Windows 2000 are available to the console? This information is not easily obtained outside of the Xbox Development Kit (XDK). The SourceForge.net Xbox-Linux project FAQ has a description of the Xbox operating system in relation to their achievements in running modified Linux distributions on the console. In explaining why they do not attempt to run Windows on top of the Xbox kernel, the project describes the Xbox O/S as lacking "memory protection and built-in sound/Video drivers". But this project is not concerned with Windows

© SANS Institute 2003, Author retains full rights.

2000 components, since they use after-market BIOS chips to run their modified Linux code without the Xbox kernel.

So where are there other clues as to the PC-compatibility of the Xbox and the O/S components available? The SourceForge.net Xbox-Linux project, in an attempt to verify PC-compatibility, was able to run Windows 2000 on top of their modified Linux distributions in a virtual machine configuration. This proves PC-compatibility to some extent, and that once the modified Linux code provides the drivers necessary for PC-type operation, Windows 2000 will run on the Xbox hardware. But once more this requires the modified Linux distribution to be run against an after-market BIOS. Again, the elusiveness of the Xbox Windows 2000 components is demonstrated by the lack of published information on the subject.

Fortunately, another Xbox enthusiast web site has published details from official XDK information they obtained. This document exposes some of the Xbox under-belly to the research community:

Xbox ROM

The XDK information describes the Read-Only-Memory as containing the Hardware Abstraction Layer, drivers for the hard drive and DVD drive, file system, and application services such as memory management and threading.

Software System Kernel

This is the previously mentioned slimmed-down version of Windows 2000 that runs the Xbox. Differences between PC-based Windows 2000 operating system include the inability to run on multiple hardware platforms and non-support for numerous simultaneous processes.

The XDK information states that non-simultaneous process includes support for multiple threads, and that programs will run in Kernel mode.

The XDK information also states that standard Windows 2000 graphical user interface (GUI) is not provided by the kernel. The GUI is provisioned by the Game developers themselves, (for the games they create and market), which would interactively load from the game disc upon system start-up. There is a component called the “Xbox Dashboard”, which is the GUI used when no game disk is present.

Also described in this information, are some of the Windows 2000 services that are not available to the Xbox kernel. Pertinent missing components include Plug and Play, Memory Page file usage, multi-processor support, and NTFS file system.

© SANS Institute 2003, Author retains full rights.

Boot up

The XDK information outlines the console initialization as the Kernel being de-compressed out of Read-Only-Memory and into the Random-Access-Memory of the device. Hardware such as the DVD drive, audio and video components are started in RAM after kernel decompression.

Program Execution

The XDK information notes an interesting aspect of the internal working of Xbox's operating system. When a game is placed into the console DVD drive, the game image is loaded into Random-Access-Memory. These images must have a special electronic sign and the kernel must confirm this sign during loading. Once in RAM, the Xbox kernel starts the game and works in tandem with operating system components provided by the game developer's DVD. This information goes on to state that these game images are not standard PC-type executable formats, and must be loaded by the special Xbox kernel. Another interesting note in this section is that there are no dynamic-link-library loads.

Networking

The XDK information states that the Xbox networking libraries included by Game developers on their products provides TCP/IP and Winsock support. This would enable a game to be played via the Internet or a Local Area network, presumably with other players of the same game. This support coupled with the consoles integrated Ethernet port makes the Xbox compatible with online play.

Thanks to the enthusiasts at xbox365.com, and their publishing of hard-to-find XDK information, a definite analysis of the inner workings of the Xbox is available. Although the Xbox uses PC-type hardware components, Microsoft has taken great care to limit the operating system used by the Xbox so that it only has what it needs for its primary functions of playing games, movies and music. It should be very difficult for malicious parties to introduce dangerous code into a standard Xbox configuration.

Xbox Security – Encryption

This paper has described the unique capabilities of the custom Xbox operating system, and its ability to limit the code that interacts with the console. This should prove that the unit is protected from un-signed code that may be malicious in nature. But what about protecting the inner workings of the console itself? And as the previous topic illustrated the online capabilities of the unit, what does Xbox do to protect its communications over the Internet?

Xbox use of encryption is best illustrated in the escapades of Operation Project X. This project describes their goal of cracking the 2048-bit RSA private

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

encryption key Microsoft uses to ensure only authorized software runs on the Xbox. The defeat of the encryption would assist their ultimate goal of running Linux on an un-modified, no-mod-chip-installed Xbox. This must be a very difficult key to crack, given that the project has released distributed computing software, similar to SETI@home, to enlist as many CPU cycles as possible in an attempt to defeat the encryption during our lifetime.

However, an MIT doctoral graduate has identified a hardware-based method for obtaining the key. Andrew "bunnie" Huang has been in the press numerous times for his analysis of Xbox encryption. He claims to have built a simple electronics board that, once soldered onto the right places, "sniffs" the key during Xbox bus transport. The research for this paper did not show any published usage (either legal or illegal) of Mr. Huang's method. Due to the purposely-limited operating system of the Xbox, using the compromised key for running un-signed software still must be very difficult.

Xbox encryption does an excellent job of protecting the console from running un-authorized code, barring any strenuous hardware modifications. But what about the use of encryption to protect Xbox online communications? To answer this question, one must determine what in the console's online interactions is worthy of the encryption overhead.

Xbox Online

With Xbox's built in Ethernet port, and the TCP/IP and Winsock support mentioned above, the Xbox is capable of connecting to the Internet. The primary reason to connect an Xbox to the Internet is to play multi-player games and download new game content. There are two methods for using an Xbox over the Internet. One involves the usage of 3rd-party software, commonly referred to as a "tunnel". This fools the Xbox into playing Local Area Network games over the Internet. Since the "tunnel" is free, and there are no fees for playing online with the "tunnel", this type of traffic would not be worthy of the encryption over-head.

The second method is Microsoft's online gaming service for the Xbox, known as Xbox Live. Since this service is subscription based, personal as well as financial information is transmitted and stored. This would be the type of online communication, that is not only worthy, but expected to be encrypted in today's online world. The Xbox Live website describes the information needed to set up a subscription, and the most pertinent ones are: 1) Full Name, 2) Billing Address, 3) Credit or Check card number. Since un-authorized access to this type of information is the beginning of identity theft, it is imperative that Xbox Live subscription information is protected.

In a preview of the Xbox Live service, the subscription information has been described as being handled with protection of personal information in mind. All authentications into the Xbox Live service, no matter which game is being

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

played, is handled through central Microsoft servers. This means that the login information, as well as the personal information associated with it, is stored and accessed by one party only, Microsoft. The preview also states that the personal information is not stored on the Xbox console itself. This information is stored on the centralized Microsoft servers and is protected by “military grade” encryption. A more recent review that compares the online offerings between Microsoft Xbox and Sony Playstation2 offers specific details of Xbox Live Internet traffic. It states that the traffic uses a custom version of IPSec to ensure that packets cannot be spoofed or modified, and that any data transmission to other Xbox Live users or the central servers is authenticated. This would indicate that Microsoft is very concerned with the protection of Xbox games and its user’s data.

The preview mentioned before goes on to say that in the future Microsoft is considering using pre-paid cards for Xbox Live purchases. This would remove the most sensitive personal information from the equation, the credit or check card number. However, a check of the Microsoft Xbox Live website does not mention this capability as being a current feature.

This paper previously discussed the usage of an after-market BIOS as a way of running un-signed code on the Xbox. This was one method of running Linux on the console. Since an active mod chip soldered onto the Xbox motherboard removes the check so that only approved code works, the question becomes can an after market BIOS affect Xbox Live security by introducing un-signed code into the stream. The answer is no, because Xbox Live is smart enough to check for the presence of the after-market BIOS. If it detects it, the console is not allowed into the Xbox Live stream.

Again, Microsoft has demonstrated its commitment to Xbox security by the inclusion of secure networking technologies in its online gaming architecture. This coupled with specialized operating system and encryption should cause consideration as Xbox being the most secure console gaming platform on the market. But is it?

Alleged/proven Vulnerabilities

Are there any published vulnerabilities for Xbox? A check of the Microsoft Knowledge Base search site shows that Xbox is not a choice in the product pull-down list. Doing a KB search using “Xbox” has the criteria bring back a few articles, none of which relate to any known vulnerabilities. Likewise, there are no bulletins posted on the Microsoft Technet Security site, nor is Xbox available as product choice in the pull-down product list.

Further research did not show any published and proven vulnerabilities. Mr Andrew Huang, who was previously mentioned as de-ciphering an Xbox encryption key, has indicated other hardware-based problems. He describes “test” solder points left onto the board that in certain methods can circumvent the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Xbox software. He also describes the usage of “fast buses” as not being enough to protect the integrity of a cipher key. His interception or “sniffing” of the fast bus is what allowed him to decipher the key. Another hardware-based issue he claims is that the boot-up sequence can be affected to by-pass the signed code check. Still another problem Mr. Huang identifies is the storage of a unique identifier on the Xbox that he believes can be mis-used to identify Xbox users on the Internet. Research for this paper did not find any published usage of Mr. Huang’s discoveries. He has limited the amount of technical detail in his public publishing to the Internet, but has released his own book outlining in detail his research in Xbox reverse-engineering and vulnerability discovery. The book was not published in time to be used as a source for this paper.

UK-based researcher Andy Green and others have discovered another hardware-based issue regarding Xbox encryption. Using a known vulnerability in the TEA algorithm, which the research team determined was used to create a particular hash, the team was able by-pass the code sign check mechanism of the Xbox operating system.

This paper’s research found only 1 software vulnerability, and it was documented as a technique to boot Linux (or any un-signed code) without the presence of an after-market BIOS. A researcher using the name Habibi Xbox found that by using a particular game’s load/save feature, he was able to induce a buffer overflow that caused his Linux boot-loader to run.

Overall, these vulnerabilities mainly revolve around the capacity to run un-signed code on the console. Due to technical constraints required to accomplish these tasks, these points would not affect the average Xbox user. At this point in the paper’s public research, no serious vulnerabilities exist to compromise the use of an un-modified Xbox online.

Xbox Modifications

As previously noted in this paper, it is possible to run un-signed code on the Xbox with the addition of an after-market BIOS. Soldering a mod-chip onto the console’s motherboard usually provides this. Once this done, all of Microsoft check mechanism’s are bypassed. Therefore it is assumed that one could load a Trojan or Virus, as well as a modified Linux distribution. Xbox owners who decide to use mod chips must be extra careful in the software they use.

Linux usage itself is outside of the scope of this paper. However, one must assume vulnerabilities can possibly exist in modified Xbox Linux distributions in relation to their corresponding PC Linux distributions. Knowledge and care should be exercised when connecting an Xbox running Linux to the public Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A recent magazine article mentioned the game load technique described in the Vulnerability section of this paper. It stated a possible benefit to booting Linux on the Xbox. The article described the ability to access the consoles hard drive via FTP to trade game progress saves with others. Does this mean that a modified (and maybe Xbox Live enabled) Xbox does accept FTP connections natively? This could have an effect on the average Xbox user who does not understand the consequences of a FTP server exposed to the Internet.

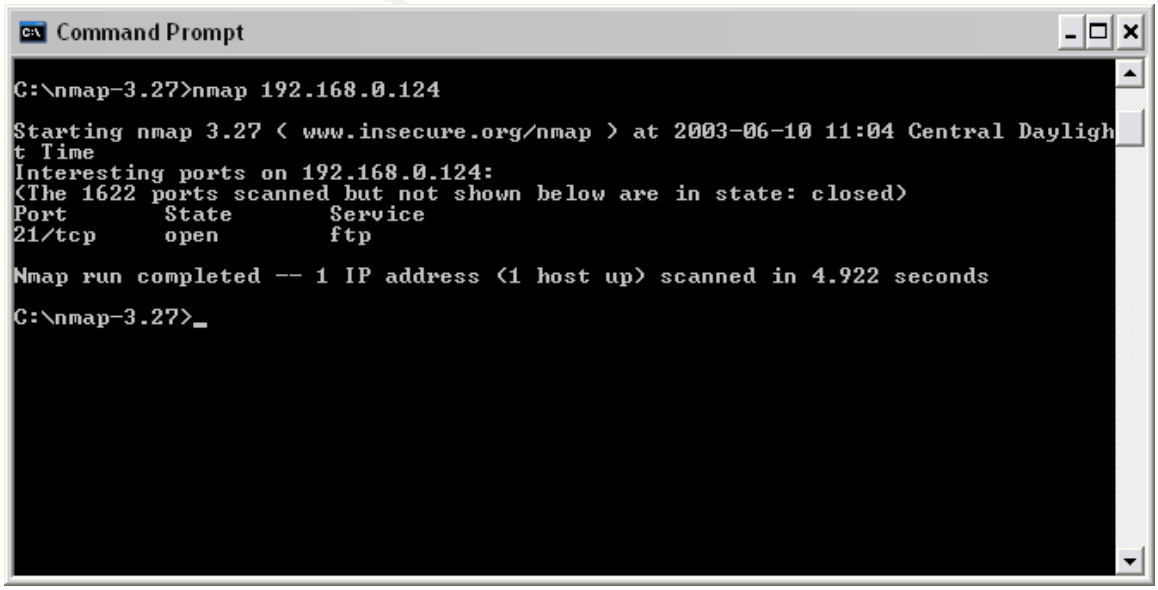
Xbox FTP

To examine the FTP capabilities of the Xbox, a mod-chip enabled Xbox was obtained for the purposes of this paper's research. Ideally, an Xbox Live enabled Xbox would better suit the analysis since that configuration reflects the majority of people who use their Xbox online. However, an Xbox Live account was not available. This type of research may be outside of the Xbox Live licensing terms.

The research Xbox was connected to a Network Address Translation (NAT) network to keep the console off of the public Internet. Without the addition of the after-market BIOS from a mod-chip, the Xbox does not automatically obtain an IP address for DHCP. Once the console is booted using the after-market BIOS, the console contacts the DHCP server on the NAT network. In this case, the console was assigned the IP of 192.168.0.124.

To attempt reconnaissance of the console's NAT IP address, nmap ver. 3.27 was used to determine any listening ports. The research for this section used part of the Chapter 6, Exercise 1 instructions from the GSEC Security Essentials Toolkit.

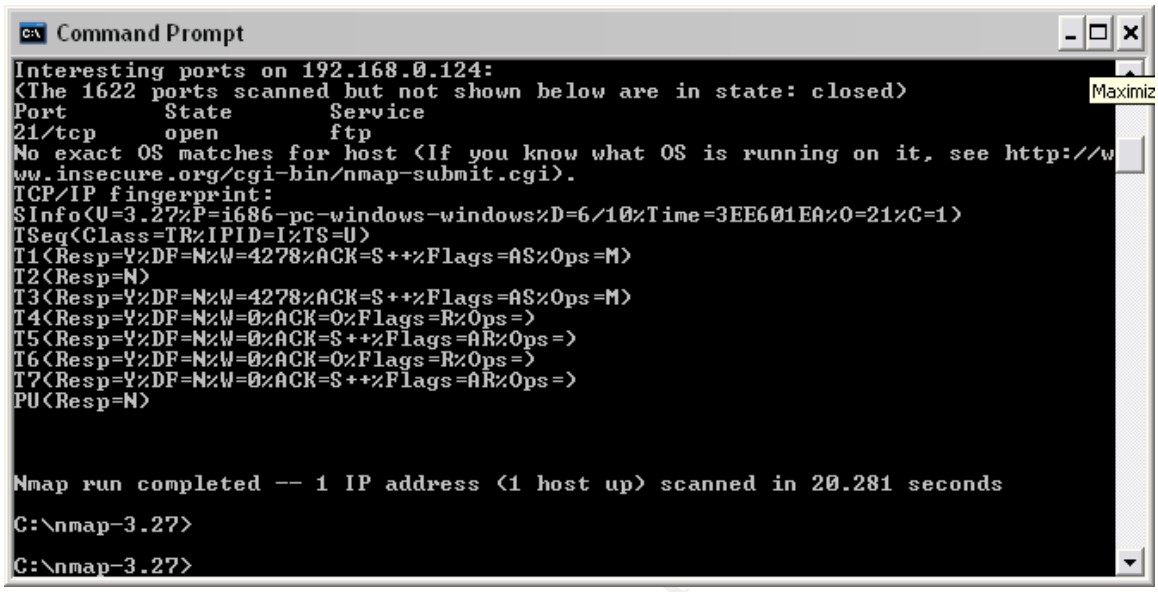
1) nmap 192.168.0.124



This scan shows that port 21 is open for FTP connections

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

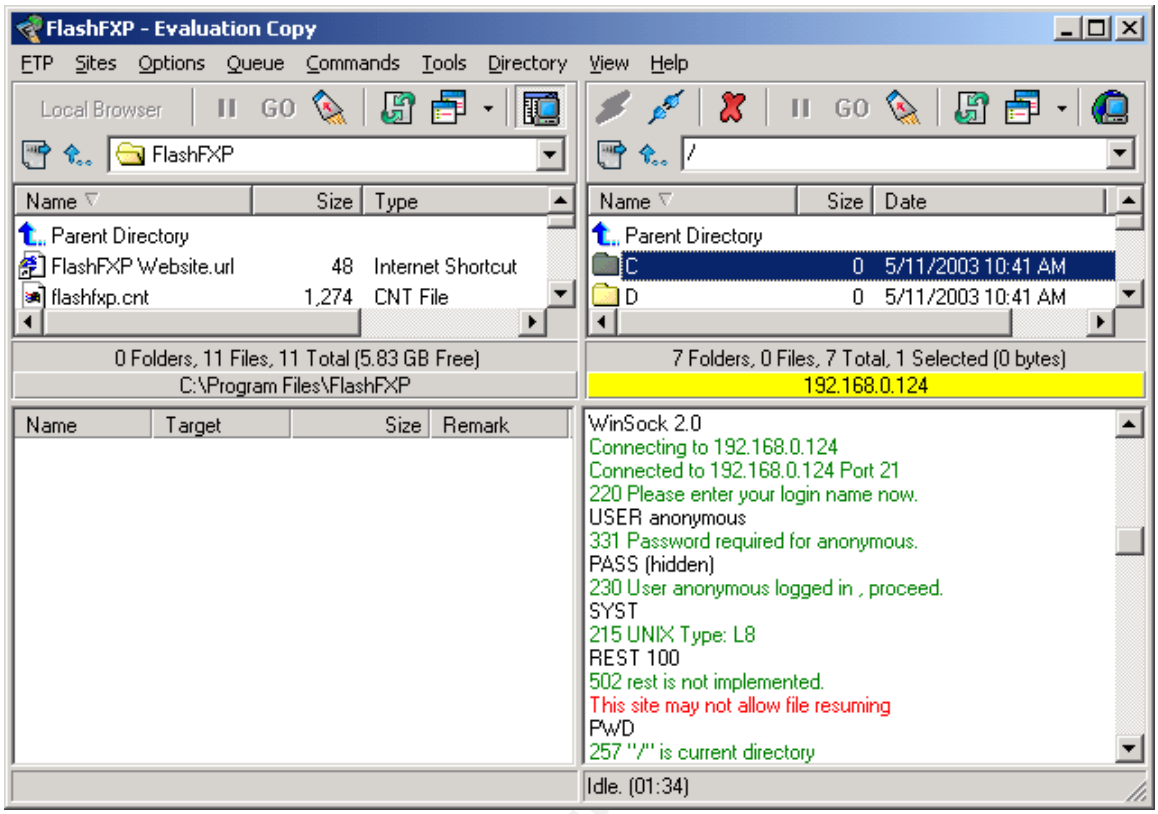
2) nmap 192.168.0.124 –O



This scan attempts to identify the operating system. Notice that nmap was unable to determine the operating system, but notice the TCP/IP fingerprint that was returned.

Nmap shows that the console is listening on the standard FTP port of 21. Now that it has been determined that console will accept FTP connections, the question lies in what type of authentication does the console do when accepting an FTP connection. Using a shareware FTP program an anonymous FTP connection was attempted to the console's IP address:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



As shown in the screenshot, the FTP program was able to connect anonymously to the console. At this point, the connected FTP user has the ability to upload or download files, rename and even delete files off of the console's partitions.

Conclusions

Overall, the Xbox demonstrates Microsoft's commitment to creating a secure entertainment device for its consumers. The console protects its components through encryption and signed keys so that only authorized code will run. Network communication between the console and central authentication and gaming serves is protected as well. The Xbox Live network is smart enough to check for the presence of an after-market BIOS to prohibit such devices from introducing un-signed code.

However, the usage of an after-market BIOS, allows all of the console's check mechanism's to be by-passed. At the same time, this allows the console to obtain an IP address from a DHCP server. If an Xbox in this configuration is placed on a public Internet connection, the unit becomes a stand-alone, anonymous FTP server. This could be a problem for users who do not understand the consequences of allowing anonymous FTP connections. An un-suspecting Xbox consumer, who uses a mod-chip after-market BIOS, could find their console's hard drive partitions filled up with illicit files by malicious FTP users who scan the public Internet for open FTP servers. Even worse, a malicious FTP user could delete or re-name critical files on the console, rendering it useless.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Calls for Analysis

Questions remain about other aspects of Xbox security. Future GSEC candidates may be able to research further on the following topics:

1) Do Xbox Live enabled consoles accept anonymous connections on FTP port 21? If this is true, then a recommended configuration by Microsoft poses serious problems for Xbox Live. This configuration says to connect the console directly into the users broadband modem. If the users ISP or modem equipment provides no incoming port blocking, Xbox Live users could be exposed to the same FTP problems as after-market BIOS users.

2) Are there any problems with console operation described in XDK?

3) Are there any special considerations for modified Linux distributions for the Xbox and their security vulnerabilities?

4) Are Mr. Huangs efforts to circumvent the hardware protection of the console a future sign towards the effectiveness of other secure hardware initiatives such as Microsoft's Next-Generation Secure Computing Base?

References

The Microsoft Corporation. "Xbox Video Game System." URL: http://www.xbox.com/system/xbox.htm (4 Jun. 2003).

XboxReporter.com. "Xbox System Specifications." URL: http://www.xbreporter.com/xbox_system_specifications.php (4 Jun 2003).

SourceForge.net Xbox-Linux Project. "Xbox-Linux FAQ." URL: http://xbox-linux.sourceforge.net/faq.php (5 Jun 2003).

Broersma, Matthew. "Hackers make Xbox into a Windows PC." 30 Sep 2002. URL: http://news.zdnet.co.uk/story/0,,t269-s2123049,00.html (Jun 2003).

Brown, Jason. "Xbox System Software Overview – official leaked document from the XDK." URL: http://www.xbox365.com/stories/xdkcomplete.shtml (5 Jun 2003).

OperationProjectX.com. "The Xbox Attack." URL: http://www.operationprojectx.com/main.asp?PageRequest=ABOUTXBOX (5 Jun 2003).

Middleton, James. "Xbox hacked with $50-worth of Hardware." 6 Jun 2002. URL: http://webactive.vnunet.com/News/1132402 (5 Jun 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Microsoft Corporation. “Create Your Xbox Live Account.” URL: http://www.xbox.com/LIVE/Accounts/YourAccount_Setup.htm (4 Jun 2003).

Leonard, Mike. “Gamewatcher Countdown – Xbox Live.” 12 Nov 2002. URL: http://www.allxbox.com/news/stories/11122002680.asp (4 Jun 2003).

Sentinel. “Xbox Live vs. Playstation2 Online.” URL: http://www.ingaming.com/articles.php?f=39&p=1 (8 Jun 2003).

Reuters. “MIT Student Foils Xbox Security.” 3 Jun 2002. URL: http://zdnet.com.com/2100-1103-931364.html (6 Jun 2003).

Xatrix Security. “New Xbox Security Cracked by Linux Fans.” URL: http://xatrix.org/article2040.html (8 Jun 2003).

LWN.net. “Security News – I Expect You To Boot Linux, Mr. Bond.” URL: http://lwn.net/Articles/26920/ (8 Jun 2003).

“Xbox Linux.” Official Xbox Magazine. July 2003 (2003): 16.

Cole, Eric. Newfield, Mathew. Millican, John. GSEC Security Essentials Toolkit. Indianapolis: Que Publishing, 2002. 125-130.

The Microsoft Corporation. “Direct Connection.” URL: http://www.xbox.com/LIVE/Connect/direct.htm (8 Jun 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.