GUIDE TO (mostly) HARMLESS HACKING
Vol. 7 No. 1
Introduction to Hacker Wargaming

Since we began running the Hacker Wargame in March 1988, so far (Oct. 1998)

we have just two winners (blips and spagheti -- GALF doesn't count because they committed a felony to get in) -- and lots of questions about how to become a winner. "Please explain keystroke by keystroke," people ask again and again.

Sorry, I can't do that for you. The problem is, when we made the Wargame easy to win, certain script kiddies came in and repeatedly erased key parts of the operating system of the Wargame computer -- which is a pain to fix.

So we decided to set up the Wargame so it was harder to use script kiddie programs. The result, sad to say, was that winners became rare.

It's pretty boring when only two people are able to not just break into but maintain control of one of our Wargame computers. (You aren't a winner unless you can maintain control.) So this Wargaming series is intended to teach you, the aspiring Uberhacker, how to rise above the level of the script kiddie. If this series is successful, you will learn how hackers such as blips and spagheti have become computer security experts instead of mere script kiddies. You will have the opportunity to follow in their footsteps by learning how to discover new computer vulnerabilities, and learning how to fix them yourself, without being told "keystroke by keystroke."

****

In this GTMHH you will learn:

*** What are script kiddies and why they are lame**
*** Why setting up your own LAN (local area network) is the best**

way to become
an Uberhacker
* What kind of hardware you will need
* How to get hardware cheap
* How to get operating system software cheap
****

What Are Script Kiddies, and Why they Are Lame

Want to know exactly what a script kiddie is? The Web site http://www.antionline.com carries some of the best news about computer break-ins. Its owner, John Vranesevich <jp@antionline.com> is a self-described hacker, and has interviewed and listened to thousands of hackers. With his permission, here we reprint his recent editorial "Facing the Age of the Script Kiddies"

In the past, a hacker was an individual who literally had to spend years to learn the inner workings of computer technology, programming, and hardware. Only then could he begin to explore possible vulnerabilities, and develop, for himself, ways to exploit those vulnerabilities, and more importantly, ways to patch them. Through out these years of learning, the hacker would develop a certain respect for the technology that he was studying, and a certain level of maturity would inherently develop as well.

Now, in present day society, with point and click utilities abound, a younger, less mature, less knowledgeable, and less respectful, generation of "hackers" have come to life. Individuals who haven't had to go through the years of learning, and study. Individuals, who because of the lack of experiencing this "learning process" have not developed the traits which once went hand in hand with the persona of "hacker". Kids who are at that age, where they have very

little self
respect, and even less respect for others. Kids who are insecure, and have
a strong desire to feel that sense of belonging. The sense of being
accepted as part of a group, and respected among their peers. The same
emotional state which once led inner city youth to gangs, is now leading
them to "hacking". Individuals who feel the ultimate sense of power in
"hacking a webpage". Their words being read by thousands of others. Their
ability to control something. The technology is not a love, but a tool to
accomplish something much more in their eyes. A tool that can be used to
gain them acceptance, a feeling of empowerment, belonging, and control. A
tool to allow them to escape the ridicule of the kids on the bus, or the
back of their parent's hand.

Oh, and I can hear people screaming "stereotyping" right now. Well,
call
it what you may. I've talked to literally thousands of these so called
"hackers" over the past 5 or 6 years. You'd be surprised at how clear of a
mold many of them come from. I am really sick of hearing "we hacked that
page to get a message out". Perhaps, in some very, very, rare cases, that
is true. But, I submit to you, the vast majority of time a hack is done
first, and a political agenda is developed after hand to help rationalize
the crime. On top of that, one hardly has to "hack a webpage" to get their
point of view told.

That's the wonder of the Internet. Everyone is an equal. Everyone has
the
opportunity to post their views, and share their thoughts. Once again,
these so called "hackers" avoid the developmental process. They don't want

to spend the time and energy necessary to create a successful website of their own. So, they maliciously exploit the work of others that have. I'm 19 years old right now. I know what it is like being upset about something, and feeling that there's no way to share that with others.

That's one of the reasons that I made AntiOnline. It's my forum. My way of expressing my views on things. To think of me, a 19 year old college drop out. Yet, my work is viewed millions of times every month. That, my little

"hacker" friends, is power. That is what the Internet is about. That's why it works. That's why it's growing.

Unless you change your ways soon, you will never be truly experiencing the wonder that technology is. To truly love technology, love how it is changing our society, bringing mankind together in a way never before experienced in the history of the human race. You'll never truly be experiencing the very thing that you feel you have ultimate control over. A

true irony indeed.

Of course, as with all things, there is hope. There are people out their hanging on tightly to the ways of old, and the true hacker identity. There are groups like L0pht, the distributed.net bovine group, and the kids down at your local high school learning visual basic.

Those are the true hackers. A desire to learn, a desire to be the first to discover something new. A true hacker mentality is something that shouldn't be thought of as a dark, mischievous thing, but perhaps, more like that of a scientist. Study, learn, experiment, and

share what you've
found with others.....
Yours In CyberSpace,
John Vranesevich
Founder, AntiOnline

Why Setting up your own LAN Is the Best Way to become an Uberhacker

OK, so you want to become more than a script kiddie? So do I. Here's what

the best hackers I know say was their route to the top: wargaming on their own and friends' LANs (local area networks). This is a study technique used by the kind of people who can slide through computer systems like ghosts wafting through walls.

"Wait! Wait!" some of you are saying. "I thought hackers learn by illegally breaking into the computers of strangers!" True, plenty of people you meet on hacker mailing lists and on IRC make out like they are computer security experts by day and computer criminals by night. There even are people who have been convicted of computer crimes who work as security experts. These guys probably are telling you the truth when they say they were foolish enough to learn their trade by committing crime.

However, crime often leads to prison, and prison is no fun. Guess what happens when bad breath cellmate "Bubba" decides you're cute? Guess what happens when your name is Kevin Mitnik and Hollywood makes a movie full of lies about you? Besides, when you break into a computer illegally, you miss out on the most fun part, which is being the guy who is fighting back!

So ... are you ready to learn about breaking into and defending computers the way the Uberhackers do it? Ready to learn how to run your own hacker wargames?

You can get started with newbie wargaming by reading the

GTMHHs on "How to
Break into Windows 95 from the Internet." (See
http://www.happyhacker.org)
These show you how to set up your Win95 box so you and your friends can
practice breaking into each others' computers over the Internet. This will
give you a good start. But this approach has some problems -- such as you
only learn newbie stuff, and strangers might find your purposely vulnerable
Win95 or Win98 box connected to the Internet -- and do terrible things to it.
If you want a wargaming technique that will take you all the way to the
top, you need to set up a local area network in your home, and get your
friends to set up networks, too. Then you can experiment with configuring
firewalls and proxy servers, getting several computers with different
operating systems working together, and trying out LAN networking techniques
such as Netware, Microsoft Network, and TCP/IP; and much more. You can
increase your fun by trading accounts on your network for accounts on your
friends' LANs and get to freely experiment with many LANs.
****
Newbie note: If you are a kid, the FIRST thing you will probably want to do
is make sure your parents understand why hacker wargaming will make you rich
and famous instead of in jail and infamous. Here's how
Paradox@kpservices.com won over his parents.

"I wrote to you a while ago about how to get my parents to accept the
fact
of their son being a white-hat hacker... You gave me the advice to show
them your article in the October issue of _Scientific American_ (which was
a masterpiece, btw) and take it from there. Right after my dad read it ...
All was well! Then, by coincidence, my best friend's Win95 box on a

vulnerable cable connection was invaded as part of a dumb IRC war he had going on... The intruders... trashed my friend's box by using Back Orifice and then proceeded to mess with the server our business page was on (along with our other e-mail addresses). My

parents ... are now security paranoid and want me to find out as much as I can about computer security. My Aunt (a Sun Microsystems employee) is getting me an Ultra 5 SPARC Workstation for Christmas too! My parents are

also buying me a copy of Windows NT and System Commander so I can run Linux

too! I'm also going to get a (secure) cable connection to the workstation in my room.

THANK YOU! THANK YOU! THANK YOU!

****

What Kind of Hardware you Will Need -- and How to Get it Cheap

"Wait! Wait!" some guys are saying. "I'm not rich enough to build my own hacker research laboratory!" Guess what, you can put together a really impressive lab for only a few hundred dollars.

Have you visited the web page of our Wargame computer http://koan.happyhacker.org? The Web pages downloaded pretty fast, right? Did you get into the guest account and make merry with all the other guys who had shells on koan? (Hint: the password for the guest account is really stupid. Even a stupid person can guess it.) Did you give the netstat command and see how many people were browsing its Web sites, making ftp connections and logged into shells all at once? Did you know that koan is a mere 25 Mhz 486 box?

Koan is so powerful because it runs FreeBSD, a Unix type of operating system, instead of Windows. (The RAM disk for the temp directory helps,

too:) Almost any Unix type operating system can take an ancient Intel-type computer and make it run fast! The 200th fastest supercomputer in the world is a bunch of PCs running Linux and hooked together in parallel, in operation at Los Alamos National Laboratories.

You can get a 25 Mhz PC, or even faster ones, for almost nothing. Because they are so common, you can find cheap used ones in the classified ads in the local paper, or buy them from computer stores that specialize in used equipment. Then install Unix type operating systems on them.

Or, for major fun, buy ancient workstation computers. You will rarely see them for sale in the classified ads of newspapers. However, you can often pick them up at auctions. Of course you need to know a thing or two about the hardware you buy at auctions, because usually you won't get to try them out before bidding on them. Many people who buy workstations at auctions figure most of them have things wrong with them. So they buy a bunch of them and then use parts from some of them to fix the others.

You would be surprised by what an ancient Sun can do. A Sun SPARC workstation running at 25 Mhz is surprisingly fast for the same reason a 25 Mhz PC is fast running some sort of Unix -- it's the Unix that makes it fast! In addition, if you want to have many simultaneous users, for example if you want to give shell accounts to many users, a Sun should be faster than a PC with an equivalent clock speed.

If you don't feel you have the hardware expertise to piece together a cheap

Sun workstation yourself, by paying a little bit more you can buy them from resellers who get them at auctions. If you can find a local auction that sells workstations, you best bet may be to go to the auction and introduce

yourself to the people you see buying hardware that you want to own. They will probably be willing to resell to you as soon as they get the equipment working.

If you can't find a cheap place to buy workstations nearby, there are two places in Albuquerque where you can get refurbished workstations: http://nmol.com/users/jcents (email jcents@nmol.com); or email Jake Garcia at jakeg@rt66.com. They pick them up at auctions of used equipment from places such as Sandia National Laboratories, where people design nuclear weapons and nanomachinery. Sorry, you won't find classified data left behind on these workstations!

Your next step in getting ready to set up your hacker laboratory is the networking equipment. How do you get your computers talking to each other? For that I recommend a 10BaseT Ethernet. This is probably the easiest network you can set up.

The hardware you will need for an Ethernet will consist of a hub, an Ethernet device for each computer you plan to network together, and either Category 3 or Category 5 Ethernet cables. The Ethernet cables look like oversized phone cables.

You can usually find a used hub for $20 or so at a used computer store. Workstations usually have an Ethernet device of some sort already built into them. However, look to see whether yours has a connector on the back that looks like a slightly oversized phone jack. If it does, great. If instead your workstation only has a connector that looks like what you use for a cable TV (round with a wire in the center), and next to it a connector that looks like the serial port on the back of your PC, you have a slight problem. You will need to buy an AUI to 10BaseT transceiver. It is a

little box with LEDs on it which hooks on one side to the thing that looks like a serial port, and on the other side has a thing that looks like a big phone jack. These are somewhat hard to find, and cost about $30 new. The electronic parts supplier Hamilton Hallmark sells them, as do many other electronics parts suppliers. You rarely will find these transceivers in computer stores because the average consumer doesn't run around networking old Unix workstations.

For PCs you usually need to buy an Ethernet card. Even new, you can buy one for only $20. The cabling costs very little, and can often be gotten for free if you pay a visit to an office building that is being renovated. I've gotten several hundred feet of Cat3 cable that way.

Once you have gotten this far, you have all the hardware you need for your hacker laboratory.

How to Get Operating System Software Cheap

Your next problem will be operating system software. One problem with buying old Unix workstations is that they generally have old operating systems for which there are many exploit programs floating around the Internet. While it may be fun for a while proving to yourself that within seconds you can break into these old boxes, pretty soon this will get boring. You will get the craving to upgrade to the latest versions of these operating systems.

This is where you may get to faint, when you find out what this costs. There are exceptions, however.

My favorite kind of used workstations is Suns. The reason I like old Suns is that you can either run them using whatever operating system it came with (either Sun OS or Solaris, which will probably be an old version and easy to break into) or you can upgrade cheaply to the latest version of

Solaris, to
Sun Linux, or Sun OpenBSD. Even a SPARC 1 can run the latest versions of
all of these! To get the latest Solaris for almost nothing, see
http://www.sun.com/developers/solarispromo.html. This offer includes the
manuals as well as a set of installation CDs. Or, you can get a version of
Linux that runs on Sun workstations (Red Hat) at
http://www.redhat.com, or
of OpenBSD from http://www.openBSD.org.

For PCs, your best bet for cheap Unix, if you are a total beginner, is Red
Hat. It is easy to install and tech support is great. There are at least
two other Linux distributions that beginners find easy to use: Slackware 3.5
(http://www.cdrom.com) and Debian (http://www.debian.com). While they are a
bit harder to install, they are easier to make secure.

You can also get a version of Solaris that will run on PCs (see above URL).

If Linux is new to you, check out
http://sunsite.unc.edu/mdw/ldp.html for
lots of beginner information. Or, start out with Trinux, at
http://www.trinux.org, for a beginner's version that doesn't require you to
repartition your hard disk (which the other Linuxes do).

If you are already a power user of Linux, and want to build a really secure

LAN, you may wish to move up to either FreeBSD
(http://www.freebsd.org or
http://www.cdrom.com) or Open BSD (http://www.openbsd.org). These operating
systems, along with Solaris 2.6 and above, are designed to resist most of
the buffer overflows that are the basis of many break-in techniques. These
BSD operating systems are more difficult to install, however.

I wish I could tell you how to get a cheap version of Windows NT Server
4.0. However, the only way I know of is not exactly legal. You may be able
to obtain a free beta copy of Windows NT 5.0, however -- keep checking out

the Microsoft Web site (http://www.microsoft.com) for opportunities.

How about LAN software? If you have decided to work with Windows only, and

don't plan on connecting your LAN to the Internet, all you have to do is cable each computer to your hub, and point and click your way through networking. As for Novell Netware -- sorry, I don't know of a cheap way to get it.

If you are serious about hacking, you will be connecting several different operating systems together on your LAN. For this I recommend using TCP/IP and making one of your computers a gateway to the Internet. This is a little harder than "Network Neighborhood" style networking. I know that because -- you will be shocked to hear this -- I am living proof that it is easy to make mistakes when setting up a TCP/IP network. Imagine that! So I'm going to devote the next Guide in this series to how to set up a LAN with an Internet gateway and both Windows and Unix boxes on it using TCP/IP. Maybe I can figure out how to explain it so it will be easier for you than it was for me.

Thanks to keydet89@yahoo.com for reviewing and contributing to this Guide.

Where are those back issues of GTMHHs and Happy Hacker Digests? Check out the official Happy Hacker Web page at http://www.happyhacker.org.

We are against computer crime. We support good, old-fashioned hacking of the kind that led to the creation of the Internet and a new era of freedom of information. But we hate computer crime. So don't email us about any crimes you may have committed!

To subscribe to Happy Hacker and receive the Guides to (mostly) Harmless

**Hacking, please email hacker@techbroker.com with message "subscribe
happy-hacker" in the body of your message.**
