Global Information Assurance Certification Paper

Name: **Jim Walker**
Assignment Version: **Version 1.3**
Title: **Be careful what is left unlocked…**
The kids may get in ...

Scope

In today's environment, computer exploits are discovered on a daily basis. With this number of exploits being researched and exploited by the pool of Black / Gray crackers on the Internet, it is important to understand and know about those that may be working to infiltrate your network. The goal of this paper is to enlighten computer and security experts to the vast community of hacker/crackers, the tools used, where they learn vulnerabilities and exploits, and where they hang out to trade exploits and knowledge.

Organized Cracking

There are numerous groups on the Internet that are dedicated to defacing and breaching the security of information systems. These organizations come from all nationalities, sexes, and all age brackets. There are a number of organized groups such as: WoH (World of Hate) , Hax0rs Lab, Silver Lords, Digital Wrappers, woot-project, and Trippin Smurfs. The two groups I concentrated on were "::woot-project:: " and "..: Trippin Smurfs :.." . The reasons for choosing these two groups was due to their increasing visibility in the cracker community and their melting pot membership. These organizations are known as defacers. In the defacer communities, there are sites on the Internet known as mirror sites that actually keep track of examples of defacements that have been submitted for archiving. There used to be http://www.safemode.org and http://www.attrition.org . These sites are still up but are no longer accepting examples of defacements. Recently, a new mirror site www.zone-h.com has come online. Zone-h started tracking new defacements as of Jan 2002. Before I go over some of the techniques and tools that today's script kiddies use to breach information systems on the internet, I should explain some of the vocabulary that you will see in the IRC chat summaries.

Terminalogy	Definition
Exploits	Programs usually written in C or Perl to exploit vulnerabilities in a system.
Crew	An organized hacker, cracker, or script kiddies group.
Defacer	A hacker/cracker that focuses on defacing web sites.
0-dayz	this slang for non-public exploits that are passed through the cracker community .
Shoutz	This is to recognize friends or crews. Ex: shoutz TrippinSmurfs and woot-project.
Banner Grab	A connection made to a port/service ie. ftp, ssh, telnet, bind, etc is running.

Root kit	A kit used to conceal back doors, used by crackers/hackers after a system has been compromised.
Owned	Having the root account login and password on a targeted machine.
Cc	Credit Cards.
Leet or leeto	Elite . ex: “leet ./script-kiddie”.
Taggin	A simple defacement of a web-page that shows someone has compromised a system but keeping the original index page intact with a small message.
Vulns	System Vulnerabilities.

::woot-project:: (http://www.dominasecurity.com/hackerz/woot-project.htm)
Members: approximately 7 members
IRC : wired.rizenet.org
Channel: #woot-project
Interview: Anto

"woot-project" is made up of approximately seven people from different international backgrounds and locations. They have members located in the UK, USA, Canada, Brazil, and New Zealand. This group considers itself to be more of a friend to the administrator and security community. I had the chance to interview "ANTO" who is a sixteen year old, young man from Canada. He explained that the most common vulnerabilities that he exploits are ssh (port 22) and telnetd on Linux.[15]

SSH vulnerability

There are a number of vulnerabilities with ssh (port 22). One vulnerability in ssh daemons (SSHv1 protocol) is that it allows possible intruders to use brute force attacks without being logged [1]. Telnet and ftp allow for brute force attacks also but the attempts to login will be logged making the potential intruder visible to a security professional. Since ssh doesn't log login attempts, it could be difficult to track or see intruders.

A newer vulnerability that was found in November of 2001 is the "CRC-32 compensation attack detector vulnerability" also known as the "detect_attack" or "deattack". This vulnerability is contained in the code that was embedded in the SSH1 protocol to address the exploitation of the weaknesses in CRC-32. As described by www.cert.org for the detect_attack vulnerability:

" There is a remote integer overflow vulnerability in several implementations of the SSH1 protocol. This vulnerability is located in a segment of code that was introduced to defend against exploitation of CRC32 weaknesses in the SSH1 protocol (see VU#13877). The attack detection function (detect_attack, located in deattack.c) makes use of a dynamically allocated hash table to store connection information that is then examined to detect and respond to CRC32 attacks. By sending a crafted SSH1 packet to an affected host, an attacker can cause the SSH daemon to create a hash table with a size of zero. When the detection function then attempts to hash values into the null-sized hash table, these values can be used to modify the return address of the function call, thus causing the program to execute arbitrary code with the privileges of the SSH daemon, typically root." [2]

There is an exploit that is available (if you know the right people) called "x2" that is specifically designed to exploit the ssh vulnerability. "x2" came out last year and within three months "x3" was introduced to the underground hacker community with more features. As of now, there is an exploit named "x5" which includes the features in "x3" plus some exploits for the BIND vulnerabilities.[14] If you see the following pattern in

your system logs, you may find that your system has been breached or at least an attempted breach. [3]

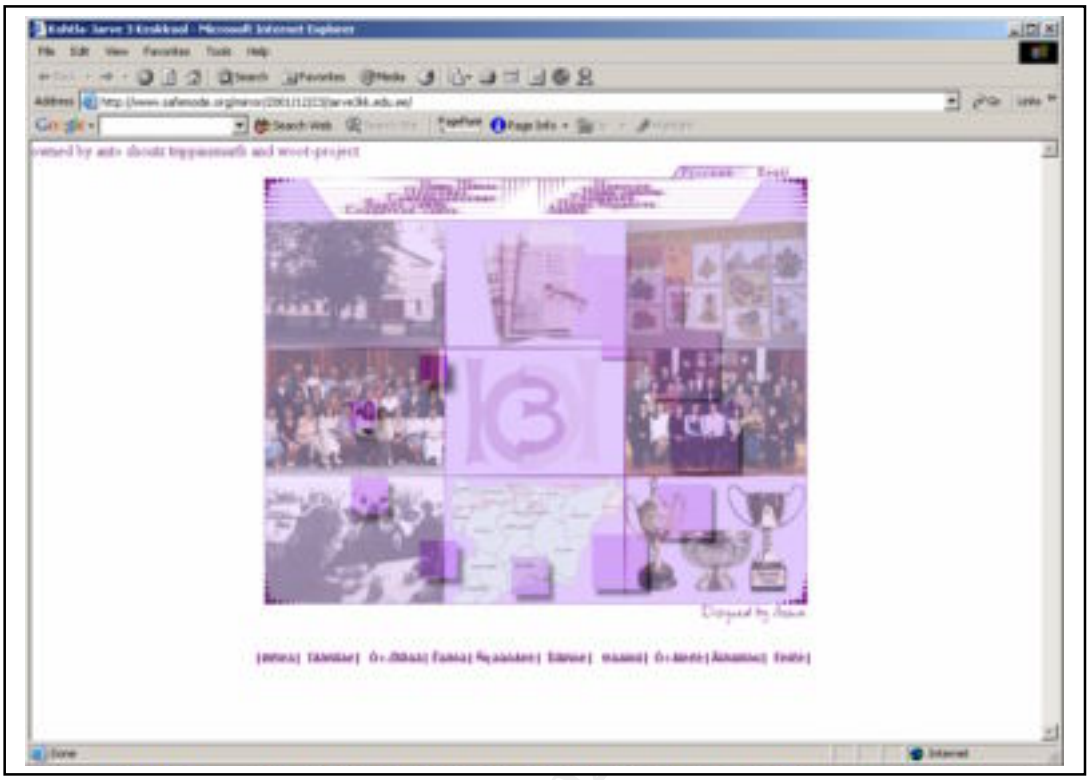
```
hostname sshd[xxx]: Disconnecting: Corrupted check bytes on input.
hostname sshd[xxx]: Disconnecting: crc32 compensation attack: network attack detected
hostname sshd[xxx]: Disconnecting: crc32 compensation attack: network attack detected
...
```

System administrators can easily remedy this vulnerability by disabling SSHv1 protocol and just allow SSHv2. This may not be a bad idea based on the large number of vulnerabilities with SSHv1. There are also vendor patches available. The main impact of this vulnerability is that root access can be obtained. Below is an excerpt from an IRC interview that was done with Anto from ::woot-project::, we discussed the vulnerability above plus some other vulnerabilities that he commonly exploits.

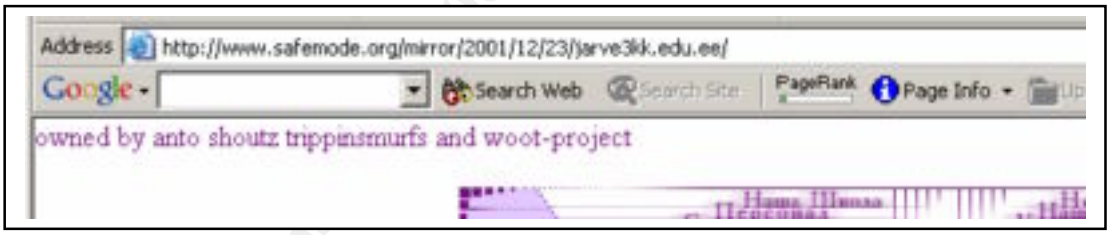
```
[20:36] <NOID> CAN WE DISCUSS VIULNS...
[20:36] <NOID> VULNS
[20:36] <ANTO> AIGHT
[20:37] <NOID> WHICH DO YOU UTILIZE THE MOST TO GAIN ACCESS TO A SYSTEM ?
[20:37] <ANTO> SSHD
[20:37] <ANTO> PORT 22
[20:37] <ANTO> THATS THE ONE I USED THE MOST
[20:37] <ANTO> BUT THERE ARE OTHERS
[20:37] <NOID> WHAT ARE SOME OF THE OTHERS
[20:38] <ANTO> TELNETD FOR REDHAT
[20:38] <ANTO> OMNIBACK FOR HP-UX
[20:38] <ANTO> SCO-POP.C FOR SCO'S
[20:38] <ANTO> SNMPXID FOR SOLARIS
[20:38] <ANTO> OR REMORSE
[20:38] <ANTO> ENOUGH?
[20:38] <NOID> WHAT ABOUT WINDOWS
[20:39] <ANTO> WINDOW IS CONSIDERED LAME AND FOR LAMERS
[20:39] <NOID> LOL ...
[20:39] <ANTO> BUT IF I DECIDE ONE DAY TO DO WINDOWS
[20:39] <ANTO> ITLL PROBABLY BE UNICODE
[20:39] <ANTO> OR PRINT BUFFER OVERFLOW FOR IIS 5.0
[20:39] <NOID> YEA... FAMILIAR WITH THOSE...
```

Interview with Anto [15]

This is an example of of ANTO's work. Anto actually is not a regular defacer. He tends to leave a little message on the index page also known as a tag rather than completely defacing your index page. There are numerous examples on www.safemode.org that show his defacements. I have included an example of his work. Please note the shoutz to his crew and his friends. [4]



This is actually an enlargement of the top of the above page showing his shoutz and stating that your box was just "owned".



TELNETD vulnerability

The telnetd program is a server for the Telnet remote virtual terminal protocol. This program has a exploitable vulnerability which causes a buffer overflow in the Telnet daemon (telnetd). [5] This vulnerability can crash a server and be utilized to gain root access to a server. http://downloads.securityfocus.com/vulnerabilities/exploits/zp-exp-telnetd.c is a working exploit which was produced by the team at http://www.team-teso.net/.[6] Team-Teso is a group that is known in the hacker/cracker/security community for finding vulnerabilities and developing examples of vulnerability exploitation. These exploits are used in the cracking community to breech systems. This exploit is supposed to work for any version of BSDI, NetBSD, and FreeBSD.

Currently, the majority of vendors have produced patches that fix this vulnerability, but the issue is that numerous administrators have not installed these updated security patches. Although these patches are available script kiddies still find this to be an exploit that can be used on systems to gain access.

::Trippin Smurfs::
Members: 13 to 15
IRC: wired.rizenet.org
Channel: #trippinsmurfs
Interviewed: Phrackman, Dalphio , tri0, Deggie

::Trippin Smurfs:: is another crew made up of approximately 18 individuals. They have members in South America, North America, Europe, New Zealand, and Asia. The founder of this group explained that the main goal was to teach each other, learn, and have fun learning. I had the privledge to talk to several members of this group and actually enjoyed the playfulness of their nature. When asked during their interviews what they wanted to do when they got older, all of them explained they wanted to do something in the field of computer security.

"Phrackman"

"Phrackman", a 18 year old young man from the United States explained that he is founder of " Trippin Smurfs". Phrackman has three loves in his life import drag racing , grafitti, and cracking/hacking systems on the internet. He also explained that he's ambition is to bring his ability to the level which includes finding vulnerabilties in satellite networks. Phrackman explained that being a cracker/hacker is truly a life-style. He orginally started the Trippin Smurfs to have a good time with friends doing something they all enjoyed. Phrackman runs a combination of Mandrake 8.1 Windows XP and Mac OS X. He has the Windows XP running on Alienware Area-51 box and the Mandrake is running on a Dell Inspirion 8100 laptop.[13]

Phrackman helped me understand that the members of Trippin Smurfs are experienced in programming everything from scanners to rootkits. A rootkit allows a cracker to have a backdoor into a box once it has been jeopardized. An example of a rootkit could be a kit called "YOYO". YOYO is a root kit which actually leaves two backdoors on a system. The first backdoor is an sshd backdoor. This backdoor will automatically load on startup and allows an experienced cracker right in to a breeched system. The second backdoor is loaded on those machines that are running a web server. YOYO.CGI is placed in the /home/httpd/cgi-bin, /usr/local/httpd/cgi-bin , /usr/local/apache/cgi-bin , /www/httpd/cgi-bin , and /www/cgi-bin/ directories. The YOYO.cgi allows a cracker to execute code on the jeopardized machine once this is installed. After YOYO installs itself it then cleans up the evidence by uninstalling the TAR file that was used to install the root kit.[7]

From talking with Phrackman, I was able to get an understanding of how he is able to hide his location while compromising machines. Phrackman uses multiple machines when cracking a system. One example of this is outlined in the chat log below. He bounces off a router to a shell account on an already jeopardized machine to another shell account on another machine. At this point, he is no longer traceable due to the activity being traced to the machines he has jeopardized and logged into.[13]

[20:41] <paraN0|d> you say you bounce of routers how do you exactly do that ?
[20:56] <PhrackMan> back
[20:57] <paraN0|d> still typing
[20:57] <PhrackMan> ok kool
[20:57] <paraN0|d> can you answer the questions above ...
[20:59] <PhrackMan> well I connect to routers via shells and bounce through routers into shells
[20:59] <PhrackMan> so on so forth
[21:00] <PhrackMan> Finding open
[21:00] <PhrackMan> routers are very easy
[21:00] <PhrackMan> with default passwords
[21:00] <paraN0|d> so telnet into a router with default passwords
[21:00] <PhrackMan> yeh
[21:01] <paraN0|d> how do you run exploits though the router though
[21:01] <PhrackMan> there is even a sight
[21:01] <PhrackMan> with default passwords
[21:01] <PhrackMan> I use the router to connect to shells
[21:01] <PhrackMan> the router
[21:01] <PhrackMan> is just my connection
[21:01] <PhrackMan> it acts as a
[21:01] <PhrackMan> connection
[21:01] <PhrackMan> like this
[21:01] <PhrackMan> I say the process
[21:01] <PhrackMan> get a wingate wingate bounce into a shell from the shell to the router
[21:02] <PhrackMan> from the router to another router to another router
[21:02] <PhrackMan> to another router
[21:02] <PhrackMan> to the shell
[21:02] <paraN0|d> wingate is a proxy server right ....
[21:02] <PhrackMan> yes
[21:03] <paraN0|d> and when you say shell what exactly do you mean
[21:03] <PhrackMan> like I connect to a shell account
[21:03] <paraN0|d> a shell account on another box
[21:03] <paraN0|d> ?
[21:03] <PhrackMan> yes

“tri0”

“tri0” who is by far the most mischievious member of the Trippin Smurfs, is a 18 year old man from New Zealand. “tri0” helped me to understand that a large number of 0-dayz exploits come from http://www.team-teso.net . Teso’s web site lists a number of exploits that are not public knowledge, which means that no patch has been built to fix the vulnerabilities they have found. The 0-day vulnerability is truly an advantage that the cracker has over the security community. If a vulnerability exists that only the crackers are aware of and a patch doesn’t exist, this could be devestating to maintaining secure systems. “tri0” explained that he has started learning more about developing exploits rather than just running other peoples code.[13]

```
[21:19] <TRIO> WAREZ
[21:19] <TRIO> FULLY, SSH IS A BIT OLD THOUGH
[21:19] <TRIO> TELNETD, OLD, BUT SOMETIMES FUN
[21:19] <PARANO|D> IT'S JUST OUT IN DEC.. 01
[21:20] <TRIO> OLD SCHOOL LIKE SPCLPD IS KEWL FUN
[21:20] <TRIO> YEA
[21:20] <TRIO> I HAD IT AGES BEFORE THAT
[21:20] <TRIO> 0-DAYZ MAN
[21:20] <PARANO|D> YEA
[21:20] <TRIO> 0-DAYZ ALWAYS GET LEAKED
[21:20] <TRIO> AND WE GET IT
[21:20] <TRIO> BEFORE REALASE DATE
[21:20] <PARANO|D> WHAT ARE THE SITES YOU WATCH TO GET INFO
[21:21] <TRIO> WWW.SECURITYNEWSPORTAL.COM EVERYDAY
[21:21] <TRIO> WWW.SECURITEAM.ORG
[21:21] <TRIO> WWW.SECURITYFOCUS.COM
[21:21] <PARANO|D> YEA
[21:21] <TRIO> I AM ON THE BUGTAQ MAIL LIST, AND VULNWATCH ONE ASWELL
```

"tri0" has began to develop a Ddos network utilizing a private exploit that one of his friends developed which they have named "wormwu.c". This code actually is a worm that utilizes the vulnerabilities with WU-FTPD (Washington University FTP daemon) such as the globbing vulnerability. [13] "File Globbing" or the glob() function has a buffer overflow vulnerability which can allow attackers to run arbitrary code. The glob() (specifically glob(3)) function is used to translate short hand notation into complete file names. It does not properly handle FTP requests that contain a tilde '~' and another special character in the pathname. [21] I have included an example that shows this vulnerability. [8]

```
FTP> OPEN LOCALHOST
CONNECTED TO LOCALHOST (127.0.0.1).
220 SASHA FTP SERVER (VERSION WU-2.6.1-18) READY.
NAME (LOCALHOST:ROOT): ANONYMOUS
331 GUEST LOGIN OK, SEND YOUR COMPLETE E-MAIL ADDRESS AS PASSWORD.
PASSWORD:
230 GUEST LOGIN OK, ACCESS RESTRICTIONS APPLY.
REMOTE SYSTEM TYPE IS UNIX.
USING BINARY MODE TO TRANSFER FILES.
FTP> LS ~{
227 ENTERING PASSIVE MODE (127,0,0,1,241,205)
421 SERVICE NOT AVAILABLE, REMOTE SERVER HAS CLOSED CONNECTION

1405 ? S 0:00 FTPD: ACCEPTING CONNECTIONS ON PORT 21
7611 TTY3 S 1:29 GDB /USR/SBIN/WU.FTPD
26256 ? S 0:00 FTPD: SASHA:ANONYMOUS/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
26265 TTY3 R 0:00 BASH -C PS AX | GREP FTPD
(GDB) AT 26256
ATTACHING TO PROGRAM: /USR/SBIN/WU.FTPD, PROCESS 26256
SYMBOLS ALREADY LOADED FOR /LIB/LIBCRYPT.SO.1
SYMBOLS ALREADY LOADED FOR /LIB/LIBNSL.SO.1
SYMBOLS ALREADY LOADED FOR /LIB/LIBRESOLV.SO.2
SYMBOLS ALREADY LOADED FOR /LIB/LIBPAM.SO.0
SYMBOLS ALREADY LOADED FOR /LIB/LIBDL.SO.2
SYMBOLS ALREADY LOADED FOR /LIB/I686/LIBC.SO.6
SYMBOLS ALREADY LOADED FOR /LIB/LD-LINUX.SO.2
SYMBOLS ALREADY LOADED FOR /LIB/LIBNSS_FILES.SO.2
SYMBOLS ALREADY LOADED FOR /LIB/LIBNSS_NISPLUS.SO.2
SYMBOLS ALREADY LOADED FOR /LIB/LIBNSS_NIS.SO.2
0X40165544 IN __LIBC_READ () FROM /LIB/I686/LIBC.SO.6
(GDB) C
CONTINUING.

PROGRAM RECEIVED SIGNAL SIGSEGV, SEGMENTATION FAULT.
__LIBC_FREE (MEM=0X61616161) AT MALLOC.C:3136
3136 IN MALLOC.C
```

There has been an exploit developed called '7350wurm' or 'wu' which was built by Team-Teso to utilize the WU-FTP vulnerabilities. 'wu' is pretty common among the cracking community. '7350wurm' can be downloaded from http://www.team-teso.net/releases.php and then find 7350wu-v5.tar.gz.[9]

"tri0's" 'wormwu.c' utilizes the '7350wurm' code to infiltrate systems. "tri0" explained that once his worm has infected a machine it loads "kaiten.c" locally to that machine. It then begins to search for other machines that are vulnerable. The "kaint.c" tool is a tool that adds a jepordized machine to an IRC chatroom. Once the machine has been added to the chatroom, commands can be sent to all the machines that are active in the controling chatroom. At this point, the infected machine is a zombie machine. "kaiten.c" source can be downloaded from www.packetstorm.net. [10]

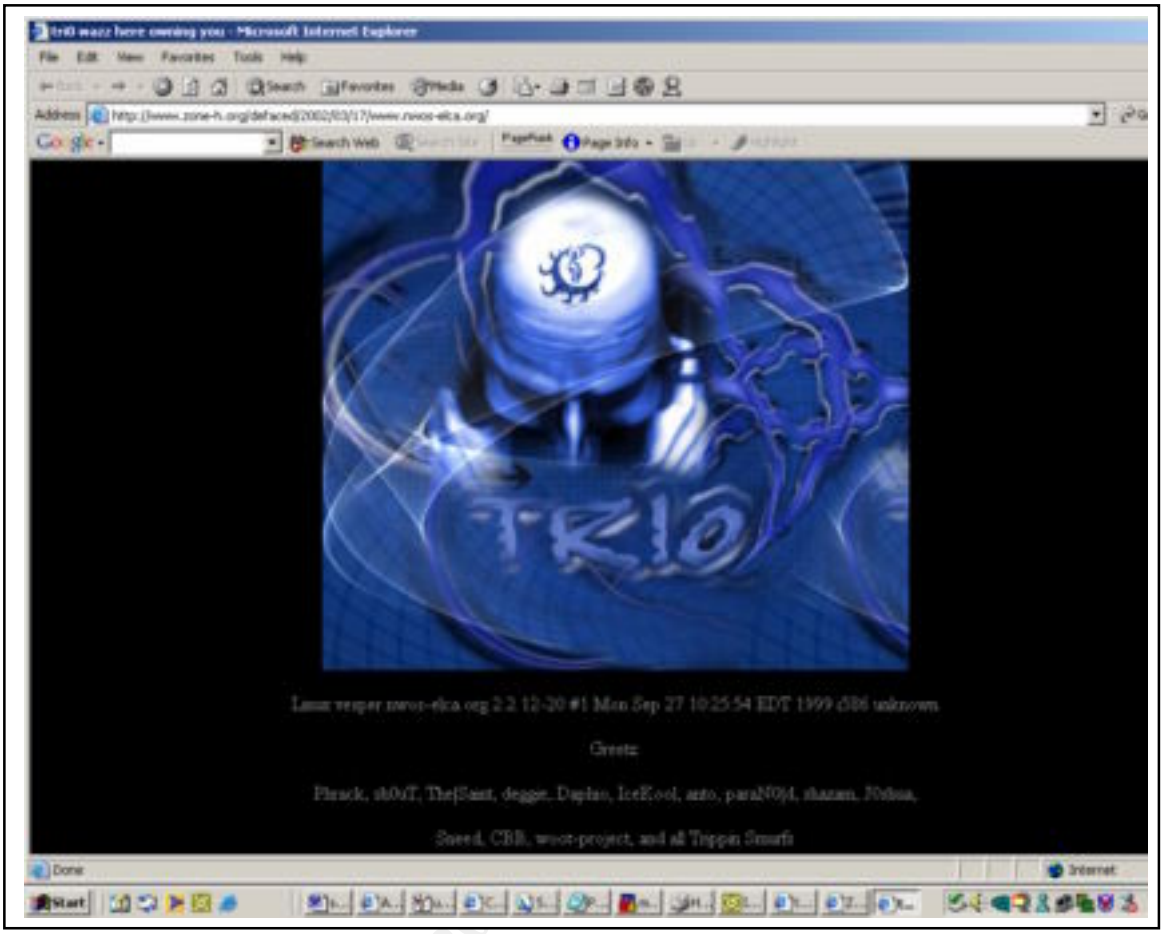
[21:24] <paraNO|D> WHAT DO YOU USE
[21:24] <tri0> HEH, IM A BUM, USED TO DEFACE A BIT, IM OUT A BIT
[21:24] <tri0> IM JUST USING WURM, TELNETD AND SOME LITTLE THINGS , WAREZ, IM MAKING A DDOS NET
[21:24] <tri0> ;-)
[21:25] <tri0> NOT DEFACING AT THE MOMENT
[21:25] <paraNO|D> SO WHAT ARE YOU USING TO BUILD YOUR NETWORK
[21:25] <paraNO|D> TFN2K
[21:25] <paraNO|D> OR
[21:25] <tri0> NOPE
[21:25] <tri0> KAITEN.C
[21:25] <tri0> ITS TIGHT MAN!
[21:26] <paraNO|D> KAITEN.C WHATS THAT
[21:26] <tri0> UMM, IT JOINS THEM ALL ON IRC
[21:26] <paraNO|D> IS THAT AN EXPLOIT
[21:26] <tri0> PROBLEM IS GETTING BUSTED BY THE IRC OPS
[21:26] <tri0> NOPE
[21:26] <paraNO|D> SO HOW DOES IT WORK
[21:26] <tri0> JUST A SCRIPT U COMPILE FROM C IN BIN, (LOL, OBIVOUSLY) AND THEN ./ ON THE B0X, AND IT JOINS UP
[21:27] <tri0> EDIT THE SRC, AND MAKE IT JOIN UR IRC SERVER, THEN BANG
[21:27] <tri0> ITS ON
[21:27] <tri0> WEEHEE, UR A PACKET KIDDIE!
[21:27] <paraNO|D> AND YOU CAN SEND COMMAND FROM THE IRC BOX
[21:27] <paraNO|D> TO ALL THE MACHINES ON
[21:27] <tri0> YEAH, WELL I MAKE IT JOIN A CHAN ON HERE, I DID HAVE ONE, BUT ITS GONE NOW, BUT THEY ALL JOIN HERE, AND U EXE COMMANDS IN THE ROOM
[21:27] <tri0> AND THEY ALL DO IT
[21:28] <paraNO|D> YEA...
[21:28] <paraNO|D> DON'T YOU HAVE TO ROOT THE BOX FIRST THOUGH
[21:28] <tri0> YEA, LOL, OF COURSE!
[21:28] <tri0> OK, HERE IS THE LOW DOWN
[21:28] <tri0> I ROOT A BOX
[21:28] <paraNO|D> OK WITH WHAT OR HOW
[21:28] <paraNO|D> DETAILS ... TRI0... DETAILS
[21:29] <tri0> I FTP TO MY LITTLE STASH OF GODDIES, AND GET THE BINARY, CHMOD +SX (BIN) THEN ./BIN, AND IT JOINS MY IRC
[21:29] <tri0> I ROOT WITH TELNETD FOR LINUX
[21:29] <tri0> WU FTPD
[21:29] <tri0> OLD SPLOITS, LIKE THE OTHER DAY I USED CFINGERD.C
[21:29] <tri0> MOUNT.C
[21:29] <tri0> ANYTHING THAT THE B0X IS VULN TO
[21:29] <tri0> CFINGERD, WU FTPD, LINUX MOUT THINGIE

"tri0" helped me understand about another exploit called "Warez". Warez is another 0-dayz exploit that targets the "dtspcd" ports. This was built to specifically target SUNOS versions 5.5 thru 5.8. The "dtspcd" service listens on port 6112. It is believed that the libDtSvc library is the component which is vulnerable to a buffer-overflow.[11] The "Warez" exploit helps to exploit this vulnerability and gain root access. This is an excerpt from the IRC interview showing the Banner of WAREZ.

```
[22:18] <tri0> [root@www warez]# ./warez -t 0
[22:18] <tri0> if you're reading this message for the first time,
[22:18] <tri0> and this file wasn't intended for you, then you
[22:18] <tri0> can assume that your whole network has already
[22:18] <tri0> been owned. now is a good time to take every
[22:18] <tri0> machine offline and completely reinstall. you've
[22:18] <tri0> been ******, so sorry you had to find it out this
[22:18] <tri0> way though... this was never meant for your eyes,
[22:18] <tri0> or for the eyes of the person who left it behind...
[22:18] <tri0> password:
[22:18] <tri0> /*
[22:18] <tri0> *
[22:18] <tri0> * This program is not to be distributed by any means.
[22:18] <tri0> * Also, it is not to be used maliciously as it is simply
[22:18] <tri0> * for educational purposes
[22:18] <tri0> Violators will be prosecuted.
[22:18] <tri0> *
[22:18] <tri0> * CDE /usr/dt/bin/dtspcd remote root exploit
[22:18] <tri0> * Version 8.3
[22:18] <tri0> */
[22:18] <tri0> The following targets are supported:
[22:18] <tri0> 1: SunOS:5.5:sun4
[22:18] <tri0> 2: SunOS:5.5.1:sun4
[22:18] <tri0> 3: SunOS:5.6:sun4
[22:18] <tri0> 4: SunOS:5.7:sun4
[22:18] <tri0> 5: SunOS:5.8:sun4
[22:18] <tri0> 6: SunOS:5.8:i86pc
[22:18] <tri0> [root@www warez]#
[22:19] <paraN0|d> whats warez do
[22:19] <tri0> hits sol
[22:19] <tri0> on the dtspcd port
```

Interview with 'tri0' [14]

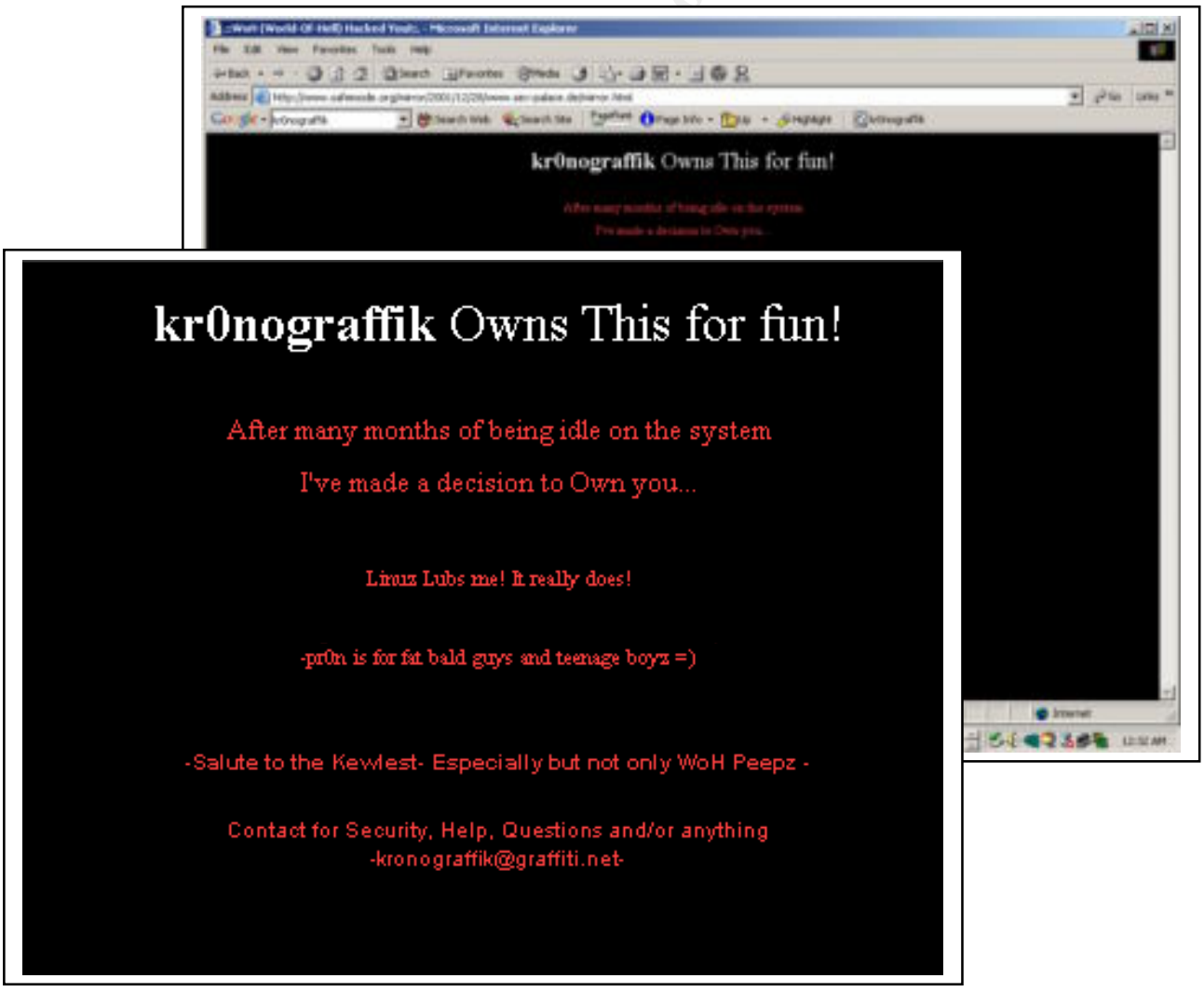
This is an example of "tri0's" defacments.



http://www.zone-h.org/defaced/2002/03/17/www.nwos-elca.org/ [23]

“Dalphio” aka “kr0nograffik”[16]

Dalphio, a 15 year old from Canada, explained that he has also been in a book written by Dan Verton titled “The Hacker Diaries: Confessions of Teenage Hackers “. Dalphio has defaced well over 400 websites he tends to utilize the Unicode exploit. Although the unicode exploit is viewed as an easy hack it is still utilized frequently. This is due to the lack of systems that have been patched. Some examples of his work can be found at www.safemode.org. [16] Although this mirror site is no longer operational, you can still view some older defacements. Dalphio used to have the handle “kr0nograffik” which is what his defacements are listed under. For example , http://www.safemode.org/mirror/2001/12/28/www.sex-palace.de/mirror.html [18] shows an example of his work defacing an adult site. At the time of this defacement Diaphio was a member of a crew called WoH or World of Hell. This crew was disbanded a few months back but a number of crackers/hackers are trying to revitalize the group. The current members are r00t,d1ckw33d, spyR0cker, FonE_TonE, and mElT. You can see the new defacements on www.zone-h.org



Dalphio explained that he looks for vulnerabilities that effect WU-FTPD, sshd, Solaris 8 lpd exploit, PHP, and a slackware BIND vulnerability.

Dalphio has built an exploit to take advantage of the sshd vulnerablity on systems. His "sshd autorooter " was able to exploit over 350 machines to help him develop a DDos network (Distributed Denial of Service network). Dalphio explained that he utilized a tool called Tribe FloodNet 2K (TFN2K) to control his 350 node DDos network. His auto-rooter was able to do a banner-grab, determine which systems were vulnerable, exploit their vulnerabilties, and then TFN2K was left for future use.[16]

TFN2K is a tool designed to allow a user to launch a coordinated attack against a specific network or host by simalatanously sending large amounts of data to these machines. TFN2K also has special features that make it difficult to recognize and filter. It allows for remotely executable commands and has the ability to send "decoy" packets while desquising the true source of the packets flooding a specific network. TFN2K also has the ability to crash or send malformed packets that will cause unstability which makes it different from its predessors TFN.[12]

[22:47] <NOID> AND TELL ME ABOUT YOUR AUTOROOTER ? WHAT DID IT DO ?
[22:47] <DAPHIO> KK
[22:48] <NOID> HIT ENTER ...SO I HAVE SOMETHING TO READ
[22:48] <DAPHIO> THE AUTOROOTER WAS AN INGENIUS PRODUCT WHICH USED THE DEATTACK EXPLOIT TO MASS ROOT MANY SYSTEMS SO I COULD BUILD A DDOS NETWORK
[22:49] <DAPHIO> :-)
[22:49] <NOID> TELL ME MORE DETAIL ABOUT HOW IT WORKED
[22:50] <DAPHIO> IT HAD A BUILT IN BANNER-GRABBER THAT WOULD BANNER GRAB SSH DAEMONS AND EXPLOIT THE VULNERABLE ONES...
[22:50] <DAPHIO> IM SURE IT'S NOT A VERY UNIQUE IDEA
[22:50] <DAPHIO> BUT IT WORKED
[22:50] <NOID> DID YOU GET YOUR DDOS NETWORK BUILT ?
[22:50] <DAPHIO> YES
[22:51] <DAPHIO> 350 NODES
[22:51] <DAPHIO> I ALSO HAD SOME CISCO ROUTERS ON IT
[22:51] <NOID> WHAT APP DID YOU USE TO CONTROL THE DDOS NETWORK
[22:51] <DAPHIO> TFN2K IM SURE YOU HEARD OF IT...
[22:51] <NOID> HOW DID YOU GET INTO THE ROUTERS
[22:51] <DAPHIO> REMEMBER THIS IS MY PAST, NOT NOW..
[22:52] <DAPHIO> WITH A CISCO 0-DAY
[22:52] <DAPHIO> HEHE

Interview with Daphio [16]

Information is king

All of the cracker/hackers I have spoken with have outlined a number of websites that they utilize to gain an upper hand when it comes to compromising a server. It is important to know that all the information that is being placed on the web for the security community to help protect their machines is also being used by the black / gray hat cracker and hacker groups to learn how to compromise systems worldwide. The following sites are sites that the majority of those I interviewed used on a daily basis. The ironic thing is that these are the same sites that security analyst also utilize.

www.securityfocus.com	**Security information – home of Bugtraq newsletter**
www.cert.org	**Computer Emergency Response Team- ran by Carnegie Mellon University**
www.securiteam.com	**Smaller security site**
www.securitynewsportal.com	**Security site**
www.vulnwatch.com	**Security and vulnerability site**
www.packetstorm.org	**This site has underground exploits ready for download**
www.team-teso.net	**Team Teso's 0-Dayz site**

Newsletters to subscribe to

ntbugtraq	**Tracks bugs with Windows NT by www.ntbugtraq.com**
Bugtraq	**News letter by www.securityfocus.com**
Vulnwatch	**News letter by www.vulnwatch.com**

Summary:

The 0-Day exploits, Warez, WU, YoYo, TFN2K and the many other tools that are custom developed for the script kiddie places the security community at a complete disadvantage. The same tools that are being utilized by the information security groups are also being leveraged against them by the information hungry groups of hackers/crackers. Information security experts need to make sure they are locking all the possible doors on their systems. After discussing the vulnerabilities with the members of these groups, they all gave me some advice which seemed profound considering it was coming from those that are compromising hundreds to thousands of systems on a weekly basis. They all said if they could give the administrators a few pieces of advice subscribe to bugtraq to keep up to date on vulnerabilities, don't leave services running that aren't needed, and don't be lazy when it comes to securing your boxes and installing patches. This is ironic coming from the very people that are testing vulnerabilities and working to get into your systems daily.

> WHAT ADVICE WOULD YOU GIVE TO ALL THE ADMINISTRATORS IN THE WORLD..IF YOU COULD OF COURSE ?
>
> PHRACKMAN:TO MAKE SURE NO NETWORK PROTOCOL IS ONLINE THAT ISNT NEEDED DONT RUN AN OVERLY COMPLICATED FIREWALL SYSTEM AND TO SIGN UP FOR A DESCENT SECURITY MAILING LIST. AND NOT TO PROCRASTINATE, OR BE LAZY CAUSE IT DOESNT PAY OFF IN THE END. [13]

> [21:45] <TRIO> WELL MY ADVICE IS, PATCH, ITS NOT HARD, SUBSCRIBE TO BUGTRAQ, SIGN UP TO UR OS VENDERS MAIL LIST, AND WATCH FOR NEW SOFTWARE EXPLOITS
> [21:46] <PARANO|D> NICE ...
> [21:46] <TRIO> AND....
> [21:47] <PARANO|D> AND WHAT
> [21:47] <TRIO> HAVE LOTS OF LOGGING SYSTEMS, A GREAT IDEA IS TO, HAVE A LOGGING SYSTEM, THAT WILL ALSO POST IT TO ANY BOX, SO THE CHANCES ARE THAT THE HACKER WONT KNOW IT, AND WONT BE-ABLE TO DESTROY THOSE LOGS
> [21:47] <PARANO|D> LOL
> [21:47] <TRIO> HEH
> [21:47] <TRIO> I READ THAT SOMEWHERE [14]

> [20:40] <NOID> IF YOU WERE TO GIVE ALL THE ADMINS OUT THERE SOME ADVICE WHAT WOULD IT BE ?
> [20:40] <ANTO> UPDATE THERE BOX'S SECURITY THE MOST THEY CAN
> [20:40] <ANTO> THERE ARE NEW EXPLOITS EVERYDAY [15]

[1] Nazario, Jose. "SSH-1 Brute Force Password Vulnerability." 5 Feb. 2001. URL: http://www.crimelabs.net/docs/sshd1-logging.txt (23 Feb. 2002).

[2] "CERT® Advisory CA-2001-35." 14 Dec. 2001. URL: http://www.cert.org/advisories/CA-2001-35.html (01 Mar. 2002).

[3] "CERT® Incident Note IN-2001-12." 07 Nov. 2001. URL : http://www.cert.org/incident_notes/IN-2001-12.html (01 Mar. 2002).

[4] URL: www.safemode.org/mirror/2001/12/23/jarve3kk.edu.ee/ (15 Mar. 2002)

[5] "CERT® Advisory CA-2001-21 Buffer Overflow in telnetd." 1 Feb. 2002. URL: http://www.cert.org/advisories/CA-2001-21.html (25 Feb. 2002).

[6] URL: http://downloads.securityfocus.com/vulnerabilities/exploits/zp-exp-telnetd.c (05 Mar. 2002).

[7] Fredrik," Linux rootkit (yoyo)." 28 May 2001. URL: http://security.alldas.org/analysis/?aid=2 (10 April 2002).

[8] SecurityFocus, "Failure to Handle Exceptional Conditions." 14 Feb 2002. URL:http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=exploit&id=3581 (14 Feb. 2002).

[9] Team-Teso, "Releases of Teso." URL: http://www.team-teso.net/releases.php (22 Mar. 2002).

[10] URL: http://packetstorm.widexs.nl/irc/kaiten.c

[11] "CERT® Advisory CA-2001-31." 3 Apr. 2002. URL: http://www.cert.org/advisories/CA-2001-31.html (3 Apr. 2002).

[12] "CERT® Advisory CA-1999-17." 3 Mar. 2000. URL :http://www.cert.org/advisories/CA-1999-17.html (3 Mar. 2000)

[13] Phrackman, IRC interview , 11 March 2002

[14] tir0 , IRC interview , 14 March 2002

[15] Anto, IRC interview ,10 March 2002

[16] Dalphio, IRC interview, 27 Feburary 2002

[17] Deggie, IRC interview, 24 Feburary 2002

[18] URL: http://www.safemode.org/mirror/2001/12/28/www.sex-palace.de/mirror.html

[19] URL: http://www.zone-h.org/defaced/2002/03/17/www.nwos-elca.org/

[20] URL: http://safemode.org/mirror/2002/01/04/colby.supernal.org/

[21] URL: http://www.iss.net/security_center/static/6332.php

[22] URL: http://safemode.org/mirror/2002/01/04/colby.supernal.org/

[23] URL: http://www.zone-h.org/defaced/2002/03/17/www.nwos-elca.org/

http://www.giac.org/GIACTC_citations.php