

## security-basics Digest of: get.123\_145

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-11/0559.html>

---

*security-basics-help\_at\_securityfocus.com*

**Date:** 11/27/04

To: [ulrich@der-keiler.de](mailto:ulrich@der-keiler.de)

Date: 27 Nov 2004 13:12:40 -0000

security-basics Digest of: get.123\_145

Topics (messages 123 through 145):

Re: Security NT Server

123 by: Robert D. Hughes

125 by: Jacob Harres

136 by: Hedges, Nigel

Re: Recovering a Sun solaris roots password

124 by: Rick Rezinis

Re: How to hide HTTP header information?

126 by: Bouncer18

135 by: P. Kane

Re: Access Controls & Router Vulnerabilities

127 by: Jay D. Dyson

Re: cd-rom write protection

128 by: Greenstein, David

130 by: Lord Soth

Re: [SECURITY-BASICS] track the user who deleted files

129 by: Lord Soth

Re: VPN to ASP a security risk?

131 by: Samuel Billas

138 by: Kevin Brown

Re: Linux firewall vs. FW-1

132 by: Gary W. Joyce

Re: Red Hat compromise

133 by: Alvin Oga

134 by: John Jasen

security-basics Digest of: get.123\_145

SecurityFocus BASICS: security-basics Digest of: get.123\_145

139 by: Ryan Russell

Reverse

137 by: R.Hoffmann

145 by: Fab

Re: E-Mail protocol error – security filter issue?

140 by: Michael Lang

[SECURITY-BASICS] .htaccess-file : password sent encrypted?

141 by: Koen4Security

Re: hard drive encryption [win98]

142 by: Berglund, Steve

Re: Multiple IPSec tunnels?

143 by: Liam Reimers

Re: IPchains and syslog configuration

144 by: Douglas J. Hunley

Administrivia:

--- Administrative commands for the security-basics list ---

I can handle administrative requests automatically. Please do not send them to the list address! Instead, send your message to the correct command address:

For help and a description of available commands, send a message to:

<security-basics-help@securityfocus.com>

To subscribe to the list, send a message to:

<security-basics-subscribe@securityfocus.com>

To remove your address from the list, just send a message to the address in the ``List-Unsubscribe" header of any list message. If you haven't changed addresses since subscribing, you can also send a message to:

<security-basics-unsubscribe@securityfocus.com>

or for the digest to:

<security-basics-digest-unsubscribe@securityfocus.com>

For addition or removal of addresses, I'll send a confirmation message to that address. When you receive it, simply reply to it to complete the transaction.

If you need to get in touch with the human owner of this list, please send a message to:

SecurityFocus BASICS: security-basics Digest of: get.123\_145

<security-basics-owner@securityfocus.com>

Please include a FORWARDED list message with ALL HEADERS intact to make it easier to help you.

--- Enclosed is a copy of the request I received.

Return-Path: <ulrich@der-keiler.de>

Received: (qmail 11946 invoked from network); 27 Nov 2004 13:12:40 -0000

Received: from mail2.securityfocus.com (205.206.231.1)

by lists.securityfocus.com with SMTP; 27 Nov 2004 13:12:40 -0000

Received: (qmail 3821 invoked by alias); 27 Nov 2004 19:26:21 -0000

Received: (qmail 3816 invoked from network); 27 Nov 2004 19:26:21 -0000

Received: from der-keiler.de (HELO mail.der-keiler.de) (195.140.232.111)

by mail2.securityfocus.com with SMTP; 27 Nov 2004 19:26:21 -0000

Received: from localhost (localhost.der-keiler.de [127.0.0.1])

by mail.der-keiler.de (Postfix) with ESMTP id D3ABF358C8A

for <security-basics-get.123\_145@securityfocus.com>; Sat, 27 Nov 2004 20:43:00 +0100 (CET)

Received: by mail.der-keiler.de (Postfix, from userid 1001)

id 266F0358C7D; Sat, 27 Nov 2004 20:43:00 +0100 (CET)

Date: Sat, 27 Nov 2004 20:43:00 +0100

From: Ulrich Keil <ulrich@der-keiler.de>

To: security-basics-get.123\_145@securityfocus.com

Message-ID: <20041127194250.GA15396@mail.der-keiler.de>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Disposition: inline

User-Agent: Mutt/1.4.1i

X-Virus-Scanned: by AMaViS perl-11

--

<http://www.derkeiler.com>

PGP Fingerprint: 5FA4 4C01 8D92 A906 E831 CAF1 3F51 8F47 1233 9AAD

Public key available at <http://www.derkeiler.com/uk/pgp-key.asc>

***attached mail follows:***

---

Date: Wed, 16 May 2001 17:20:44 -0500

To: "++WayanS" <way@semarang.wasantara.net.id>, <SECURITY-BASICS@SECURITYFOCUS.COM>

Best place to start is by downloading MS's white paper on securing NT. There's also C2 security config information for NT 4. A step by step is really way beyond the scope of this group though, since that would be at least a 100 page document ;)

-----Original Message-----

From: ++WayanS [mailto:way@semarang.wasantara.net.id]

Sent: Tuesday, May 15, 2001 8:59 PM

To: SECURITY-BASICS@SECURITYFOCUS.COM

Subject: Security NT Server

hi,  
i have nt server  
i want to know and check security of my nt server

what can i do to check this  
please, help me to tell me step by step trik and tips

thank for all  
regard,  
++WayanS  
Yang terpenting, Selalu setia

*attached mail follows:*

---

Date: Wed, 16 May 2001 15:39:33 -0500  
To: ++WayanS <way@semarang.wasantara.net.id>, SECURITY-BASICS@securityfocus.com

Oh yeah...forgot a couple,

[http://www.nmrc.org/faqs/nt/nt\\_sec12.html](http://www.nmrc.org/faqs/nt/nt_sec12.html)  
<http://www.telemark.net/~randallg/ntsecure.htm>

Regards,  
Jacob

>Date: Wed, 16 May 2001 15:22:17 -0500  
>To: ++WayanS <way@semarang.wasantara.net.id>,  
>SECURITY-BASICS@securityfocus.com  
>From: Jacob Harres <jharres@smc.omnes.slb.com>  
>Subject: Re: Security NT Server  
>  
>Check out:  
><http://www.ntsecurity.com/>  
><http://www.enteract.com/~lspitz/nt.html>  
><http://www.securityfocus.com/frames/index.html?focus=microsoft>  
><http://www.google.com/search?q=NT+Security+Checklist>  
><http://www.google.com/search?hl=en&lr=&safe=off&q=%22NT+Security%22>  
><http://www.google.com/search?hl=en&lr=&safe=off&q=%22Hacking+NT%22>  
><http://www.google.com/search?hl=en&lr=&safe=off&q=%22Hardening+NT%22>  
><http://www.google.com/search?hl=en&lr=&safe=off&q=%22Windows+NT+Security%22>  
><http://www.google.com/search?hl=en&lr=&safe=off&q=%22NT+Security+Guide%22>  
>  
>Also, the NT4 Resource Kit has a C2 configuration tool.  
>  
>Regards,

>Jacob

>

>

>

>At 01:58 AM 5/16/01 +0000, ++WayanS wrote:

>>hi,

>>i have nt server

>>i want to know and check security of my nt server

>>

>>what can i do to check this

>>please, help me to tell me step by step trik and tips

>>

>>thank for all

>>regard,

>>++WayanS

>>Yang terpenting, Selalu setia

=====

Jacob Harres

1-713-513-3143

PKI Operations Manager

SLB Network Solutions

Geoquest Tower, Houston TX

PGP Key ID: 0x919A4D04

=====

***attached mail follows:***

---

To: SECURITY-BASICS@SECURITYFOCUS.COM

Date: Wed, 16 May 2001 21:53:39 -0400

Hi Wayans,

A good place to start would be to purchase some books on the subject, many of which have already been listed in a variety of Security Focus mailing lists. Two books that can help are:

- Windows NT/2000 Network Security by E. Eugene Schultz
- Securing Windows NT/2000 Servers by Stefan Norberg

www.cert.org has a good supply of security modules which will also help you with securing NT systems. (most in PDF format)

Hacking Exposed 2nd Edition by Joel Scambray, Stuart McClure and George Kurtz also has some good information on the NT and 2000 sections. Visit their site at [www.hackingexposed.com](http://www.hackingexposed.com) for links to some other resources that might assist you.

Alternatively do as most others have done – just do a web search for "NT Security Documents" etc. on a

variety of search engines, that will also help.

Nigel H

-----Original Message-----

From: ++WayanS [mailto:way@semarang.wasantara.net.id]  
Sent: Wednesday, 16 May 2001 11:59 AM  
To: SECURITY-BASICS@SECURITYFOCUS.COM  
Subject: Security NT Server

hi,  
i have nt server  
i want to know and check security of my nt server

what can i do to check this  
please, help me to tell me step by step trik and tips

thank for all  
regard,  
++WayanS  
Yang terpenting, Selalu setia

***attached mail follows:***

---

To: SECURITY-BASICS@securityfocus.com  
Date: Wed, 16 May 2001 13:52:02 -0700

I am not aware of a way to enter single user mode without a root passwd.  
Something else you can try if you have access to another sun or a linux box  
is to remove the physical hard drive and mount it into a system where you  
have mount priveleges, then mount it and modify the root entry in the shadow  
file so that the crypt is no longer, like so

```
root:crypttext:...\nroot::...
```

of course, it is much nicer to boot from cdrom.

rick

-----Original Message-----

From: Nir Simionovich [mailto:nirs@sanctcom.com]  
Sent: Wednesday, May 16, 2001 1:50 AM  
To: SECURITY-BASICS@securityfocus.com  
Cc: endap@ireland.com  
Subject: Re: Recovering a Sun solaris roots password

Hi There,

Well, there are a couple of ways to getting in without the root password.

1. Single User Mode

When the system boots up, press the Stop and the "A" buttons together, this will halt the machine

and give you a prompt. At that point, simple type "boot -s", this will enable you to enter a single user mode, root privilage and no password.

2. If single user mode doesn't help

Get a Solaris 2.5 CD set, put the first CD in, and then do a "Stop+A".

At that point type in the prompt,

"boot cdrom -s". This would boot the CD to single user mode. Then you could mount the filesystem on

the machine, and change the password in the /etc/passwd or /etc/shadow manually.

I personally prefer Solaris 2.7 to any of the others, but that is a matter of personal taste. Although, I will usually prefer Linux. Here is an Idea, why not Install Mandrake Linux for SPARC on that machine, sure would be a nice challange :-)

Best regards,

Nir Simionovich

Linux/Security Specialist

Sanctcom.com – Security by Design

-----  
Linux is not an OS – It's a way of life  
-----

----- Original Message -----

> *Hello,*

>

> *I recently obtained a Sparc5 box secondhand, unfortunately I have no  
> passwords to the box including the root password. From bootup I determined  
> that the box is running solaris 2.5. Is there any way that I can get  
access*

> *to the box. Im not concerned about the data on the box. I may be able to  
get*

> *my hands on a copy of solaris 2.5/2.6 but the machine does not boot from  
the*

> *CD.*

>

> *Should I be looking at installing solaris 7 or 8, is 2.5 very dated?*

>

> *any help would be appreciated.*

>

> *Endap*

> email : endap@ireland.com  
>  
>  
> \*\*\*\*\*  
> *This message may contain information which is confidential or privileged.*  
> *If you are not the intended recipient, please advise the sender*  
*immediately*  
> *by reply e-mail and delete this message and any attachments*  
> *without retaining a copy.*  
>  
> \*\*\*\*\*  
>

**attached mail follows:**

---

To: "Francois Pepin" <frpepin@attglobal.net>, "Security-Basics List" <security-basics@securityfocus.com>  
Date: Wed, 16 May 2001 16:23:42 -0700

use an app called Proxymatron

it allows you to change your html header info.

----- Original Message -----

From: "Francois Pepin" <frpepin@attglobal.net>  
To: "Security-Basics List" <security-basics@securityfocus.com>  
Sent: Tuesday, May 15, 2001 9:25 PM  
Subject: RE: How to hide HTTP header information?

>  
> > *Wouldn't that depend on the CLIENT, and not the SERVER !?*  
> > *He seems to be trying to hide the info sent with the "GET"*  
> > *request, not the server's response to the request.*  
>  
> *Hum, no not really.*  
>  
> *I don't care a whit if people know that I'm using IE 5.5 SP1 here. But if*  
> *people just need to ask for any of the pages on my webserver to know that*  
> *I'm using IIS or Apache, then it gets a lot quicker to see which set of*  
> *exploits to try to use.*  
>  
> *Of course, security by obscurity is never enough. If they want my server,*  
> *they'll try the exploits for all of them. If they're just looking for a*  
> *vulnerable server, someone will end up trying an exploit that works on my*  
> *machine if it's not secure.*  
>  
> *Francois*  
>

>

***attached mail follows:***

---

Date: Wed, 16 May 2001 19:05:26 -0700 (PDT)  
To: Francois Pepin <frpepin@attglobal.net>

On Wed, 16 May 2001, Francois Pepin wrote:

> *I don't care a whit if people know that I'm using IE 5.5 SP1 here. But if*  
> *people just need to ask for any of the pages on my webserver to know that*  
> *I'm using IIS or Apache, then it gets a lot quicker to see which set of*  
> *exploits to try to use.*  
>

See my opinion of this has been that it really doesn't make it any quicker. I mean figure, say I'm a script kiddie just looking for web servers to take down. I'm going to have my scripts to take out Apache servers and my scripts to take out IIS servers.

I type in the name of my apache script and hit enter. Doesn't work, so I type in the name of my IIS script and hit enter. Lets also say that one doesn't work... I likely move on to another server.

Thing is there is just such an obscene number of poorly secured web servers out there (as is proven on a daily basis ... only a really modivated individual is going to even bother to go above and beyond rocking simple exploits. Again, in my opinion in the case of someone more modivated you have bigger concerns that them finding out the server type from the GET request.

As well, I wouldn't sweat it too hard as compared to worrying about your server being patched and making sure your security parctices are on point.

Pete

***attached mail follows:***

---

Date: Wed, 16 May 2001 16:57:24 -0700 (PDT)  
To: Security-Basics List <security-basics@securityfocus.com>

-----BEGIN PGP SIGNED MESSAGE-----

On Wed, 16 May 2001, Nicholas & Anthony McKenzie wrote:

> *Has anyone got any good links on the above topics?*

Sure.

Links on Router Vulnerabilities

<http://www.google.com/search?q=%22Router+Vulnerabilities%22>

Links on Router Access Control

<http://www.google.com/search?q=%22Router+Access+Control%22>

--Jay

(( \_\_\_\_\_  
)) )).- "There's always time for a good cup of coffee" -. >=====<---.  
C|~|C|~| (>----- Jay D. Dyson --- jdyson@treachery.net -----<) | = |-'  
'\_'`\_'`\_'`----- "Get in. Sit down. Hold on. Shut up." -----'`-----'

-----BEGIN PGP SIGNATURE-----

Version: 2.6.2

Comment: See <http://www.treachery.net/~jdyson/> for current keys.

iQCVAwUBOwMF19CClfiU/BIVAQFGNwP+OlHsiQaUC5TBUq7fY7qF5s7Cd6P9Tldw  
R0mxXyogETCIa7ssJj3CX1WGrNnLKFlnzL9QD3/VSCGnby6jv9ra4Rje0In+Ze2h  
rlGzEhaJivm0pn9oCn0L5n2SNtcLXtqTvsV+j9ArbM2WraDm2eezxefZbVTumCAD  
BhVlhx3IaqY=

=uqvs

-----END PGP SIGNATURE-----

***attached mail follows:***

---

To: 'Andrew Jones' <Andrew.Jones@meggitt.demon.co.uk>, 'Bandi' <05.08@web.de>, "'SECURITY-BASICS@  
Date: Wed, 16 May 2001 17:03:30 -0400

Lessons from the past – this approach has been used  
in the early days of computing (Early 80s) for floppy disk protection  
of games and other software. But people found ways to defeat the protection  
every time  
Finally the software industry stopped protecting the floppy disks  
The same will happened again. There is no protection in the world  
invented by one person that cannot be defeated by another person given  
enough  
time and money (Or motivation)

David Greenstein

-----Original Message-----

From: Andrew Jones [mailto:Andrew.Jones@meggitt.demon.co.uk]  
Sent: Wednesday, May 16, 2001 3:55 AM  
To: 'Bandi'; SECURITY-BASICS@SECURITYFOCUS.COM  
Subject: RE: cd-rom write protection

Ok, flame me if u want

I think that the method of CD Rom protection is by inserting bad sectors into the disk that the program itself can skip over but any CD copying software fails on. It is becoming more common on Software and Music CD's. I have heard of a few programs out there which can just do a straight copy of a disk but have not as yet found them. Things like Easy CD Creator test the sectors as they copy so bang - bad sector = failed burn = wasted cd.

Hope this helps.

Andrew Jones

Hi friends!

I heard some guys talking about some pc-games on cd-roms protected from being copied. I would like to know more about that. What do this protections and how can one get around em? I am not searching for cracks or what those pseudos used to call it. I would like to know more about the technic of covering data in that way. Could anyone help?

Thanks in advance!  
Bandi

***attached mail follows:***

---

Date: Thu, 17 May 2001 03:22:47 +0200  
To: Bandi <05.08@web.de>

Hi,

Well, fun as this subject is (cd protections), there is nothing magical about it.

There are sites like [www.mediaworld.com](http://www.mediaworld.com), and [www.gamecopyworld.com](http://www.gamecopyworld.com) that have some descriptions on various CD protections, but they usually don't explain how they work. Neither visiting any vendor's site will help you understand the methods used.

One of the methods someone already mentioned is the use of "bad sectors" if you will. This was customary with diskettes, and for a while was used

for  
CDs as well, but it's far from a protection. Modern burning softs and hardware can cope well with such "bad sectors", and they never contain any useful information.  
Some other methods are label checkings, file format and size checkings (many times these files are screwed and have a VERY large size), and basically any type of illegal TOC (table of content).  
Most of the above can actually be cracked in a matter of minutes (I know, I have done it a few times).  
There are however some better ways of protecting against copying. Stuff such as very special digital mastering is used to create some kind of digital signature on the target CD (this sig can't be reproduced by normal burning

hardware, even if it can be read), that is used when the game is run to decrypt the executable in runtime. This basically means that crackers will have to get an original copy of the game, decrypt the executable and probably make some patch.  
Other than that, there is not much that can be done, and as it seems, even this is hardly enough.

The best places to learn about this stuff is crackers sites (or "reverse code

engineers", which many of them claim to be heh)

try:

<http://cdchecks.cjb.net/> (a friend's site..)

Or just make a good old fashion web search for this stuff.

Let me just say that finding an exploitable piece of code and writing an exploit for it is a much more interesting thing to be doing, and probly a bit harder to manage (sometimes..)

LS

Bandi wrote:

> *Hi friends!*  
>  
> *I heard some guys talking about some pc-games on cd-roms protected from*  
> *being copied. I would like to know more about that. What do this*  
> *protections and how can one get around em? I am \_not\_ searching for*  
> *cracks or what those pseudos used to call it. I would like to know more*  
> *about the technic of covering data in that way.*  
> *Could anyone help?*  
>  
> *Thanks in advance!*  
> *Bandi*

**attached mail follows:**


---

Date: Thu, 17 May 2001 03:06:53 +0200  
To: wwieser@gmx.de

Wouldn't it be easier to create an alias for rm and incorporate it in a new shell script that manages the wastebasket (with the proper privs) ?  
Sounds a better idea than to change the rm command.

LS

wwieser@gmx.de wrote:

```
> ...I know, this is more likely something for secprog but I just have to
> make sure no one really adds the code proposed on this list to his
> /bin/rm command.
>
> On Tuesday 15 May 2001 05:03, Russell wrote:
>> In my rm binary, I re-coded it and put in the lines before it unlink'd the
>> file. you go like
>>
>> char c;
>> rmfile = open(to_be_deleted, O_RDWR);
>> nfile = open(to_be_saved, O_RDWR | O_CREAT);
> ...forgot 3rd arg for open()...symlink vulnerability!...
>> lseek(nfile, 0L, 0);
>> while (c != '\0')
>> {
>> c = getc(rmfile);
>> write (nfile, (char) c, 1);
> .... (char*)...
>> }
>> close(rmfile); close(nfile);
>>
>> i typed it up fast so they're may be some errors, but add that to the rm
>> source [...]
> Sorry, but what to hell is that??
> A new super-slow copying routine with the side effect that it stops in
> binary files once a nul-char is read? No, don't add this to rm.
> Use something like this to copy the file to be removed into a wastebasket
> directory. (copying using a 4kb buffer):
>
> /* returns 0 on success; !=0 on error */
> int save_it(const char *to_be_deleted,const char *to_be_saved)
> {
> int destfd;
> const ssize_t buflen=4096; /* or use `#define buflen (4096)' */
> char buf[buflen];
> ssize_t done;
> int error=0;
```

```

> int srcfd=open(to_be_deleted,O_RDONLY);
> if(srcfd<0) { fprintf(stderr,"failed to open %s: %s\n",
> to_be_deleted,strerror(errno)); return(1); }
> /* to_be_saved is something
> * like /home/user/wastebasket/^basename of to_be_deleted` */
> destfd=open(to_be_saved,O_WRONLY | O_CREAT | O_TRUNC | O_NOFOLLOW,0600);
> /* O_NOFOLLOW so that symlinks don't get followed. */
> if(destfd<0) { fprintf(stderr,"failed to open backup file %s: %s\n",
> to_be_saved,strerror(errno)); close(srcfd); return(1); }
> for(;;) {
> ssize_t rd=read(srcfd,buf,buflen);
> if(!rd) break; /* eof */
> if(rd<0) /* read error */
> { fprintf(stderr,"error reading in %s: %s\n",
> to_be_deleted,strerror(errno)); ++error; break; }
> for(done=0;;) {
> ssize_t wr=write(destfd,buf+done,rd-done);
> if(wr<0) /* write error */
> { fprintf(stderr,"error writing to %s: %s\n",
> to_be_saved,strerror(errno)); ++error; goto breakout; }
> done+=wr;
> if(done>=rd) break;
> }
> } breakout;;
> close(srcfd);
> if(close(destfd))
> { fprintf(stderr,"error closing %s: %s\n",to_be_saved,strerror(errno));
> ++error; }
> return(error);
> }
>
> Don't know what you would like to do when copying fails.
> Note: the code above should work, I used code like this several times
> but I cannot give any warranty (especially not for some typo as this
> was not copy-and-pasted but quickly coded again).
>
> Oh, and `basename' works like this:
> char *basename(const char *path)
> {
> char *ptr=strrchr(path,'/');
> return(ptr ? (ptr+1) : path);
> }
>
> To get the home dir, have a look at the man pages of getpwent() and
> getuid(). You may use something like
> ....getpwent( ..sorry man page not at hand... );...
> char to_be_saved[PATH_MAX+1]
> int rv=sprintf(to_be_saved,PATH_MAX,"%s/wastebasket/%s",
> pwd->pw_home,basename(to_be_deleted));
> if(rv>=PATH_MAX-1) /* PATH_MAX in <linux/limits.h> */
> { ...error: name too long; to_be_saved contains invalid string; don't go on }

```

>  
> > *char \*a;*  
> > *sprintf(a, "/bin/mv -f %s", rmfile);*  
> *....what about second file arg (destination) to mv?...*  
> > *system(a);*  
> *If you fear a buffer overflow with sprintf(), use*  
> *snprintf(buf,len,format,args).*  
> *However, system() is not the best thing for security...*  
>  
> *.... And now when you've read all this, note that it is of limited use if*  
> *someone deletes the file in some other user's home dir (first e-mail on*  
> *this topic). In my proposal, the waste basket is in /home/user/wastebasket*  
> *because we may not make it world-writable as anyone could otherwise*  
> *delete other user's files in the waste basket. Another proposal would be to*  
> *use /wastebasket in the root dir, set the sticky bit on it (chmod +t, I*  
> *think) and create the files in the waste basket with 0600 perms (as I do*  
> *above).*  
> *In any case, Antonio cannot get a copy of the deleted file back unless*  
> *he is root as we have to deny read/write access to files in the waste basket*  
> *for all but the file owner for security reasons.*  
> *(And we cannot keep the owner when copying into the waste basket as the*  
> *chown() sys call would require root privs...)*  
>  
> *wwieser*

***attached mail follows:***

---

To: "Jeffrey Wilkinson" <secfocus@bedrox.com>, <SECURITY-BASICS@securityfocus.com>  
Date: Wed, 16 May 2001 23:36:10 +0200

First I would start of by checking the "security" of the ASP. What steps have they taken to protect its customers? Do you trust their solution? Then I would look at my organisation and see where the weakest link is? Is it at my network or theirs? How would a possible attacker attack me? For the attacker to get to you he needs to penetrate the ASPs defences. Perhaps a FW, but he could be another customer (depending on the setup by the ASP), the he needs to get to a machine that has the possibility to reach your network. Hopefully the ASP only allows the servers that you need to work on access to do that (is the tunnel is up that is.). Say that the attacker get on the Citrix server, he now needs some tools to get to you. These tools should not be on the server. After this the attacker needs to bounce of your workstation to get to your servers. You have some internal security as well? You should be paranoid in this business but to me it sounds like there are simpler ways to get to your information. If this way is the most likely, (after you done your survey of your security), then do as you said: Put it on the DMZ.

I would recommend you to have a talk to your ASP and go thru your thoughts and worries. They should take the first step to secure you! You are the customer.

Don't know if this helped,

Samuel Billas

-----Original Message-----

From: Jeffrey Wilkinson [mailto:secfocus@bedrox.com]

Sent: den 16 maj 2001 03:33

To: SECURITY-BASICS@securityfocus.com

Subject: VPN to ASP a security risk?

Company A developed its own software for in-house use, and later decided it could earn revenue by allowing other companies in the same field to use the software as well. Company A has a T-1 to the internet and allows outsiders to run applications on its in-house server via a Citrix session. In other words, Company A is functioning as an ASP.

The recommendation from Company A's network administrator is to let each desktop at Company B that needs to use the application, start a Citrix session and open its own VPN connection to the ASP (Company A).

My concern is once a VPN connection is established, there is a path from A's network into B's network to desktops behind B's firewall. Therefore, if Company A gets hacked from the outside, the intruder has access to Company B's network as well.

I don't like the proposed solution, and am thinking more along the lines of having a VPN server sitting out in the DMZ make the VPN connection, and have the clients point to that server as the gateway. Perhaps that server could also run NAT to add another layer of security?? That would mean a hacker on A's network would have to get to our DMZ, get thru NAT, then get past our firewall, before gaining access to our LAN.

Any suggestions on how to secure this-- and what additional hazards are posed with the connection to A's network-- would be most welcome.

***attached mail follows:***

---

To: "Jeffrey Wilkinson" <secfocus@bedrox.com>, <SECURITY-BASICS@securityfocus.com>

Date: Wed, 16 May 2001 22:57:48 -0400

What you want is a VPN/Firewall hybrid that can apply firewall rules inside the tunnel (Note: Not all VPN/Firewalls can apply firewall rules inside the tunnel, but rather just to non-VPN traffic). Also, some VPN clients

include firewalls with the client software. Of course, none of this will \*guarantee\* 100% security, but nothing ever is. This model would give you the best protection while maintaining functionality. I don't know that the solution you proposed would really add much security, but maybe I don't understand exactly what you're describing.

HTH  
Brownfox

-----Original Message-----

From: Jeffrey Wilkinson [mailto:secfocus@bedrox.com]  
Sent: Tuesday, May 15, 2001 9:33 PM  
To: SECURITY-BASICS@securityfocus.com  
Subject: VPN to ASP a security risk?

Company A developed its own software for in-house use, and later decided it could earn revenue by allowing other companies in the same field to use the software as well. Company A has a T-1 to the internet and allows outsiders to run applications on its in-house server via a Citrix session. In other words, Company A is functioning as an ASP.

The recommendation from Company A's network administrator is to let each desktop at Company B that needs to use the application, start a Citrix session and open its own VPN connection to the ASP (Company A).

My concern is once a VPN connection is established, there is a path from A's network into B's network to desktops behind B's firewall. Therefore, if Company A gets hacked from the outside, the intruder has access to Company B's network as well.

I don't like the proposed solution, and am thinking more along the lines of having a VPN server sitting out in the DMZ make the VPN connection, and have the clients point to that server as the gateway. Perhaps that server could also run NAT to add another layer of security?? That would mean a hacker on A's network would have to get to our DMZ, get thru NAT, then get past our firewall, before gaining access to our LAN.

Any suggestions on how to secure this-- and what additional hazards are posed with the connection to A's network-- would be most welcome.

*attached mail follows:*

---

Date: Wed, 16 May 2001 20:39:59 -0500  
To: "Security Basics" <SECURITY-BASICS@SECURITYFOCUS.COM>

If Checkpoint is on a hardware appliance like a Nokia it's a lot more robust than a software only firewall like Linux or even checkpoint on a

pc or sparc. If latency is an issue a hardware appliance is probably a better solution.

"Network Computing" recently a comparison/review of several leading firewalls including checkpoint, Linux on redhat and Cisco PiX.

-Gary

-----Original Message-----

From: Mário" Behring [mailto:mariobehring@yahoo.com]

Sent: Tuesday, May 15, 2001 7:11 PM

To: Security Basics

Subject: Linux firewall vs. FW-1

Hi all,

I would appreciate any information regarding the pros and cons of adopting a Linux built-in firewall for a company with 500 nodes network rather than a Firewall-1 or other paid firewall.

Thanks in advance.

Regards.

Mario

---

Do You Yahoo!?

Yahoo! Auctions - buy the things you want at great prices

<http://auctions.yahoo.com/>

***attached mail follows:***

---

Date: Wed, 16 May 2001 18:37:35 -0700 (PDT)

To: Lisa Bogar <lbogar@gemini.oscs.montana.edu>

hi lisa

first set of suggestions/comments...

Redhat is a sitting duck for script kiddies..

- rh-6.2 has a bind-8.2.2 problem... unless you patched it to  
bind-8.2.3

- if its been re-installed guess we cant poke around inside to  
see how they got into it in the first place BEFORE all that activity

## SecurityFocus BASICS: security-basics Digest of: get.123\_145

- you should apply all patches as of the date of the redhat cdrom install
  - better to be blind and apply all patches than the way around...blind not to apply the patches...
- you should separate "insecure" login from a more secure server
  - even if it is behind the firewall
  - pop3/imap, ftp, telnet, ppp all belong on an insure server away from the rest of the servers
    - better still to setup secure pop3/secure imap
    - use ssh for secure ftp
    - dont use telnet at all..no point to it
  - add a special firewall/gateway for ppp users ( make sure the login and passwds is different ( from the secure server
- www, smtp, log, backups servers should NOT have any user logins...
  - for users to create webpages, have them work on those insecure servers with user logins....
  - than have a ascript scp the changes over to the real web server
- all user workstations on a different ethernet cable

those are a good starters ?? and doesnt cost a dime to implement ??  
- just set up some and implement server/network access policy

have fun  
alvin

On Wed, 16 May 2001, Lisa Bogar wrote:

>  
> *I received this message from a consultant in town on Friday. I work at*  
> *the University and he was looking for some suggestions. Thought someone*  
> *might be able to shed some light on how the person got into the box and*  
> *also how one might monitor this compromise. I have already told him to*  
> *reinstall.*  
>  
> *Thanks,*  
> *Lisa*  
>  
>  
> *Here is the chronology I was given.*  
>  
>  
> *Lisa,*  
>

> *Here is a long winded chronology of our little computer break in. Thank you  
> for your help.  
> Mack*

>  
>  
> *On Monday, May 7 at 1:30 AM my client's computer was broken into.*

>  
> *Our system is a Red Hat Linux v6.2 kernel version 2.2.14-5.0. It was a  
> fairly standard installation with HTTP, FTP, SMTP, IMAP, and NNTP, and other  
> standard INET services. The system was placed behind a FlowPoint FP2200-22  
> SDSL router/firewall with NAT. The ports allowed through the router were 21  
> (FTP), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3) and 143  
> (IMAP). Internally, we use Samba for file and printer sharing.*

>

--- deleted ---

***attached mail follows:***

---

Date: Wed, 16 May 2001 21:16:08 -0400  
To: Lisa Bogar <lbogar@gemini.oscs.montana.edu>

On Wed, 16 May 2001, Lisa Bogar wrote:

> *On Monday, May 7 at 1:30 AM my client's computer was broken into.*

>  
> *Our system is a Red Hat Linux v6.2 kernel version 2.2.14-5.0. It was a  
> fairly standard installation with HTTP, FTP, SMTP, IMAP, and NNTP, and other  
> standard INET services. The system was placed behind a FlowPoint FP2200-22  
> SDSL router/firewall with NAT. The ports allowed through the router were 21  
> (FTP), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3) and 143  
> (IMAP). Internally, we use Samba for file and printer sharing.*

I think the only one of those that has a root compromise is DNS.

There are security concerns with ftp, telnet, samba, pop3 and imap as well.

You may want to report this to sans.org and certs, and see what they say.

It does sound like it was rootkitted.

--  
-- John E. Jasen (jjasen1@umbc.edu)  
-- In theory, theory and practise are the same. In practise, they aren't.

*attached mail follows:*

---

Date: Wed, 16 May 2001 21:27:52 -0600 (MDT)  
To: Lisa Bogar <lbogar@gemini.oscs.montana.edu>

On Wed, 16 May 2001, Lisa Bogar wrote:

>  
> *I received this message from a consultant in town on Friday. I work at*  
> *the University and he was looking for some suggestions. Thought someone*  
> *might be able to shed some light on how the person got into the box and*  
> *also how one might monitor this compromise. I have already told him to*  
> *reinstall.*  
>  
<snip>  
>  
> *Our system is a Red Hat Linux v6.2 kernel version 2.2.14-5.0. It was a*  
> *fairly standard installation with HTTP, FTP, SMTP, IMAP, and NNTP, and other*  
> *standard INET services. The system was placed behind a FlowPoint FP2200-22*  
> *SDSL router/firewall with NAT. The ports allowed through the router were 21*  
> *(FTP), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3) and 143*  
> *(IMAP). Internally, we use Samba for file and printer sharing.*

Unless it was patched, there were root holes in both your FTP and DNS server software. There are very easy to use exploits for both of those.

Ryan

*attached mail follows:*

---

To: security-basics@securityfocus.com  
Date: Qua, 16 Mai 2001 23:28:01

Hello ALL,

I have an executable file under linux that was writed using C. But I don't have the source code of it.  
There is any program that, given an executable file as parameter, its returns the source code?

Thanks in advance.

Hoffmann  
MailBR - O e-mail do Brasil -- <http://www.mailbr.com.br>  
Faça já o seu. É gratuito!!!

*attached mail follows:*

---

To: "R.Hoffmann" <ronzani@linuxbr.com.br>, <security-basics@securityfocus.com>  
Date: Thu, 17 May 2001 21:10:25 -0400

Could you do a whereis [program name].c? Maybe that will lead you to the source file. If the source code was deleted, the only way to get to it would be to disassemble the compiled program using a disassembler. Even then, you wouldn't get all of the true source.

Run a search for the program name on <http://www.google.com> . You may find it there!

=====  
Fab  
fsiciliano@earthlink.net  
"The only true wisdom is in knowing you know nothing."  
-Socrates

----- Original Message -----  
From: R.Hoffmann <ronzani@linuxbr.com.br>  
To: <security-basics@securityfocus.com>  
Sent: Tuesday, January 16, 2001 11:28 PM  
Subject: Reverse

: Hello ALL,  
:  
: I have an executable file under linux that was writed using C. But I  
: don't have the source code of it.  
: There is any program that, given an executable file as parameter, its  
: returns the source code?  
:  
: Thanks in advance.  
:  
: Hoffmann  
: MailBR - O e-mail do Brasil -- <http://www.mailbr.com.br>  
: Faça já o seu. É gratuito!!!

*attached mail follows:*

---

Date: Thu, 17 May 2001 09:16:30 +0200  
To: Bill Schultz <BSchultz@foundationsoft.com>

Bill Schultz wrote:

> *Hi,*  
> *We use Exchange 5.5 (SP4) for our e-mail. Recently, a few outgoing*  
> *e-mails are being flagged (not delivered) with the following error message:*  
>  
> *A mail message was not sent due to a protocol error.*  
>  
> *550 5.7.1 <user@user.com>... \*\*\* We do not accept spam \*\*\**  
>  
> *note - (the <user@user.com> has been modified, but contains an internal*  
> *e-mail address).*  
> *The message is coming from an internal user, and is sent directly to one of*  
> *our clients (i.e. not spam). I am fairly new at this, and can't find*  
> *anywhere where we have restricted security for this particular user or*  
> *message recipient. There aren't any special restrictions for this recipient*  
> *under Internet Mail Service Connections/Mail Filtering, Routing or Security.*  
> *Does anyone have some ideas on what would cause this, where else to look,*  
> *etc...? I am unaware of any recent security changes that would prompt this*  
> *issue, but we haven't had the issue prior to about 3 weeks ago.*  
>  
> *Thanks!*  
>  
> *Bill*

Hi Bill

You have an 550 SMTP Error Code that says Relaying Denied ... and the Enhanced Delivery Code from Exchange 5.7.1 says : 5.x.x = Permanent Failure, x.7.1 = Delivery not authorized , Message refused.

theres your Problem ... 8)

have fun !

ps: Check accept mail from Permissions for this account !

Greetz Mike

***attached mail follows:***

---

To: <Security-basics@securityfocus.com>  
Date: Thu, 17 May 2001 10:17:38 +0200

Hi,

I'm using Apache and for some pages I've created a "secure" site.

I've placed an .htaccess file and all's working well.

But, I'm wondering..the username and password, are they sent in plain text or in an encrypted format?

Does anyone have some more information regarding this topic?

Greetings,

Koen

*attached mail follows:*

---

To: Security Basics <Security-basics@securityfocus.com>, 'Langa Kentane' <evablunted@earthling.net>  
Date: Thu, 17 May 2001 17:11:58 -0400

I would recomend E4M (Encryption 4 the Masses). It uses well known algorithms. It works on just about all flavors of Windows and it is FREE. It's also very easy to set up. After installing, you "mount" volumes (which look like removable drives) and can be set up as ".vol" files on your existing file system or you can dedicate an entire partition (2GB limit) to an encrypted volume.

<http://www.e4m.net>

> -----  
> *From: Langa Kentane[SMTP:evablunted@earthling.net]*  
> *Sent: Wednesday, May 16, 2001 2:39 PM*  
> *To: Security Basics*  
> *Subject: hard drive encryption [win98]*  
>  
>  
> -----BEGIN PGP SIGNED MESSAGE-----  
> *Hash: SHA1*  
>  
> *Can anybody recommend some freeware or shareware hard drive*  
> *encryption software.*  
> *Please can you also list the pro's and con's of the software [your*  
> *opinion]*  
>  
> *Thanks a mil*  
>  
> *Langa Kentane [CCNA CCSA MCSE CNA]*  
> *\_\_ \_ Tel: +27 11 443 7467*  
> *//(\_)\_ \_ \_ \_ \_*  
> *//\_//\_ \_\//^ \//*  
> */ \_ \_ / \_ / \_ / \_ \ \_ / \_ / \_ \*  
> *\*\*\* THE CHOICE OF A GNU GENERATION \*\*\**  
> <http://evablunted.nav.to/>

>  
> -----BEGIN PGP SIGNATURE-----  
> Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>  
>  
> iQA/AwUBOwLWBbaBmUoKQx8tEQJ0xACg40+TYRM6y8FVNerLVC+D8paIuM0AoJLq  
> OykiqjS20vIorvrZvgUa+gn  
> =wp5x  
> -----END PGP SIGNATURE-----  
>

***attached mail follows:***

---

To: "'security-basics@securityfocus.com'" <security-basics@securityfocus.com>  
Date: Thu, 17 May 2001 15:03:05 -0700

David and Tony,

Perhaps you should look into implementing IPSec VPNs using BSD firewalls.

We use this method here at UIA and we have run up to 8 concurrent IPSec tunnels in a star-type WAN configuration over one T1. It's not the bandwidth that limits the number of tunnels, but your hardware.

You can inexpensively implement IPSec with BSD by using an older machine such as an old Pentium or PII (which will do packet filtering just fine, even at 133 MHz). Here is a good page to begin your research:

<http://www.kame.net>

--Liam

Liam Reimers, Systems Programmer  
ULTIMATE Internet Access, Inc.  
909-482-1634 800-982-6898  
<http://www.uia.net>

-----Original Message-----

From: Kirtley, Tony [SMTP:Tony.Kirtley@jacobs.com]  
Sent: Wednesday, May 16, 2001 12:19 PM  
To: 'Johnson, David'; 'security-basics@securityfocus.com'  
Subject: RE: Multiple IPSec tunnels?

David,

I have run more than one tunnel on slower connections than a T-1. The problem with your home connection may be that the other end of the tunnel may only accept one tunnel from a single IP address. This is assuming that your router is NATing and that you are trying to connect multiple tunnels

to  
the same destination.

I guess I didn't give you an answer, just shed some more light on the question. I have a similar problem connecting more than one tunnel to a Cisco VPN concentrator. I have heard that there is a setting in the concentrator that will let you do it, but my administrator hasn't found it. Anyone else have experience in this?

Tony

-----Original Message-----

From: Johnson, David [mailto:DJohnson@IronMountain.com]  
Sent: Tuesday, May 15, 2001 12:23 PM  
To: 'security-basics@securityfocus.com'  
Subject: Multiple IPSec tunnels?

Hello again,

Can anyone tell me if it is generally possible to run multiple IPSec tunnels  
(for VPN) through a single T1?

The reason I ask is that my Linksys router at home will only pass one tunnel  
at a time. Is most higher-end equipment able to handle multiple tunnels?

What I'm wanting to do is to rent a conference room at a hotel to have a class for employees of our company. I want to be able to tap into the hotel's T1 and allow everyone to access the home network via VPN from the single connection provided by the hotel.

Does this sound feasible?

Thanks

David Johnson

***attached mail follows:***

---

To: ExpliciT <langak@freemail.absa.co.za>, Security Basics <Security-basics@securityfocus.com>, L  
Date: Thu, 17 May 2001 17:17:31 -0400

On Thursday 17 May 2001 16:48, ExpliciT babbled:  
> -----BEGIN PGP SIGNED MESSAGE-----  
> Hash: SHA1  
>

> *How do I tell syslog to send logs to a different file and not*  
> */var/log/messages?*  
>

edit /etc/syslog.conf

--

Douglas J. Hunley (Linux User #174778)

<http://hunley.homeip.net/http://linux.nf/http://www.kicq.org/>

if i knew what i was doing, life would be so much more boring