white hat briefings

(version 0.1a) 022703 ...heh

white hat briefings

A bit of c0de for good faith.....

```
char code[] =

"\xeb\x30\x5e\x89\x76\x2d\x31\xc0\x88\x46\x08\x88\x46\x0b\x88\x46"
"\x2c\x89\x46\x39\xb0\x0b\x8d\x5e\x09\x89\x5e\x31\x8d\x5e\x0c\x89"
"\x5e\x35\x89\xf3\x8d\x4e\x2d\x8d\x56\x39\xcd\x80\x31\xc0\xb0\x01"
"\xcd\x80\xe8\xcb\xff\xff\xff\x2f\x2f\x62\x69\x6e\x2f\x73\x68\x20"
"\x2d\x63\x20\x65\x63\x68\x6f\x20\x73\x61\x76\x65\x20\x61\x20\x62"
"\x75\x67\x2c\x20\x6b\x69\x6c\x6c\x20\x61\x20\x77\x68\x69\x74\x65"
"\x68\x61\x74";

int main()

{
        int (*funct) ();
        funct = (int (*) ()) code;
        (int) (*funct) ();
}
```

white hat briefings

Quick, run patchadd on your staff!!!!

Security Advisory MA-2003-01 - CISSP Trojan

Security Advisory MA-2003-01 CISSP - Trojan Security Certification

Original Release Date: Thursday January 16, 2003
Last Revised: --
Source: --

Systems Affected

- Information Security Community
- Information Technology Employers
- Information Security Consultants

Overview

It has recently been identified that The International Information Systems Security Certification Consortium (CISSP) has developed and released a potentially destructive trojan application, which masquerades as a valid standard for professional certification in the field of information security.

Employers are encouraged to recognize the CISSP as a trojan certification.

white hat briefings

Ummm, can u plz show me how to get

Date: Sun, 05 Jan 2003 00:33:19 -0500
Subject: Re: solttdb

Hi,

We spoke once before about mysql thing. I was hoping you could send me that old solttdb binary you did a review on. Those polska lsd hos' stuff always gives me weird, tough to fix compile errors. That thing is like 4-5 years old, but i'd still like to have it in my archive (yes i know the source is on their page) Thanks.

BTW any new reviews on the way ?

** WHAT HE REALLY MEAN IS, "CAN YOU PLZ FIX THE CODE, **
** I REALLY WOULD LIKE TO OWN SO SERVERS THAT I FOUND **
** ..... CAN YOU SHOW ME MORE ./ TECHNIQE, PLZZZZ" **

white hat briefings

SANS/GIAC Update Version 9
February 22, 2002

Table of Contents:

.....

1) ALERT - GCIA Exam Compromise

I regret to report that a training organization in China is copying slides from the SANS Intrusion Detection in Depth Training and has illegally and ineptly attempted teaching this material. In addition, we now have evidence they are circulating past GCIA exam questions as a part of a GCIA certification exam preparation course.

……

.. poor mr. northcutt, seems to be a bit upset that someone is making money off of network traces him and his goons captured on some l33t honeypots. lets do this!

#rm -rf Stephen_Northcutt_-_The_SANS_Institute &

white hat briefings

$ matters to the lame no matter how they get it

http://www.counterpane.com/crypto-gram-0302.html

…….

“The bug secrecy position is a lot easier to explain to a layman. If there's a vulnerability in a system, it's better not to make that vulnerability public. The bad guys will learn about it and use it, the argument goes. Last month's SQL Slammer is a case in point. If the hacker who wrote the worm hadn't had access to the public information about the SQL vulnerability, maybe he wouldn't have written the worm. The problem, according to this position, is more the information about the vulnerability and less the vulnerability itself. “

……

heh, why mr. Schneier really supports full disclosure is because he can make $$ off the underground. Like many other security firms, counterpane stands and waits for something to leak in order to make a profit….

white hat briefings

f00d for thought =)

Your high priced security sans certified engineer's plane ticket: $1500

Your high priced security sans certified engineer's time: $100/hour

RealSecure nodes all over your networks: $200,000

Getting it in the ass by 0day: **Priceless**

the funnies

Q: whats the difference between a sans certified person and a corpse?

A: a couple of minutes!!!

white hat briefings

do you know where your servers are?

The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus

….jeeze, gimmie a break. The experts are who again? Oh yeah, they are the people who site in a committee with their .ppt slides and discuss whether or not if nfs exported to the world is the real threat….or umm maybe null sessions, or umm anonymous ftpd, or umm so they can spam you and your mom with the joke of a poster they put togther.

white hat briefings

The real threat

XSS

…for those of you l33t folks, cross site scripting is security experts nightmare!!!!!!!

white hat briefings

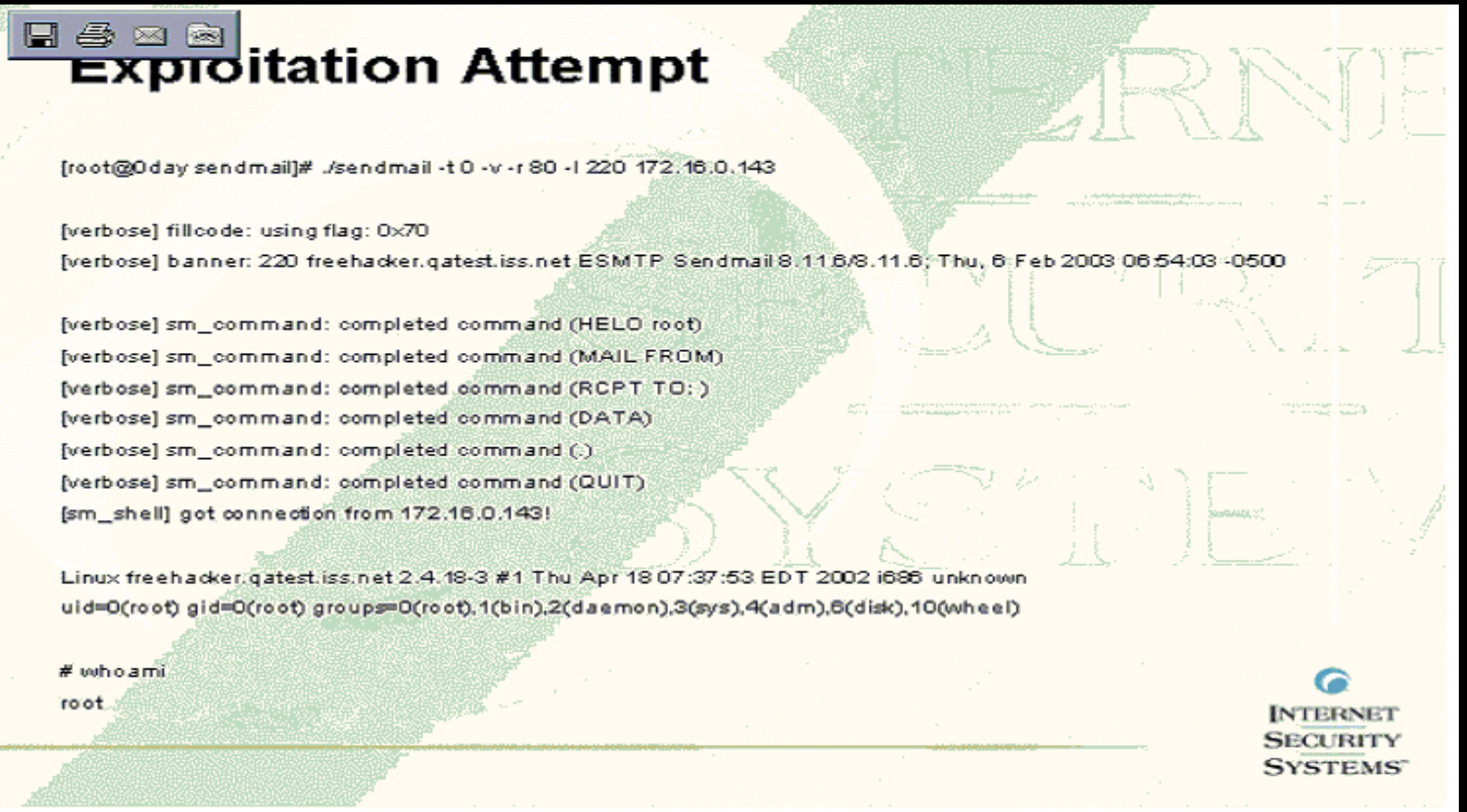
INTERNET | SECURITY | SYSTEMS™

Advisories

Internet Security Systems Security Advisory March 3, 2003
Remote Sendmail Header Processing Vulnerability

Internet Security Systems Security Advisory March 3, 2003
Snort RPC Preprocessing Vulnerability

- ohoh, iss put two whitehat money making advisories out, (on the same day!) Run express update on all your nodes.....



do i really need to say more .....

white hat briefings

mOnk@shaolin:~/docs/phrack

File Edit Settings Help

```
#phrack ARIS THREATCON MONITOR v1.0
-----------------------------------
current threatcon is: 3 / possible 7

Threatcon History for March, 2003
Date          Description                  [ ][ ][ ][ ][ ][ ][ ]
----------    ---------------------------  ---------------------
03/01/2003    Beginning                     X  X
03/03/2003    Lord Duke sendmail catastrophe X  X  X  X  X
03/06/2003    malicious hacker tsao is owned X  X  X  X
03/07/2003    threatbar released (phew!)    X  X  X

open: Permission denied
```

h0h0h0h0.....

Life ain't nothin but bitches, money, and root.

nuff said

white hat briefings

Brought to you by the letters “rm,” and his buddies “kill -9”

more to come……. Fo sho……..heh!