
GOBBLES
SECURITY
HACKERS
THAT
HACK!@%!!

THE CISSP
aka
Why The Infosec INDUSTRY IS A FUCKING JOKE

WITH COLLOBARATION
FROM

THE PHRACK
HIGH COUNCIL


calling all whitehats
step into the oven

WOLVES AMONG US

G-CON ONE

WOLVES AMONG US

MEXICO

owned by

#PHRACK

pr0ud supp0rt3rz 0f pr0j3kt m4yh3m

```
# grep ssh /home/thievco/.bash_history
   ssh -l ryan mail.securityfocus.com
   ssh -l ryan mail.securityfocus.com
```

POINT #1 (uno)

JUST BECAUSE SOMEONE HAS A JOB WITH A SOCALLED SECURITY COMPANY IT DOES NOT MAKE THEM A SECURITY EXPERT

LOOK AT ME
I FINISHED
PRESCHOOL AND
NOW I'M READY
TO TEACH AT
HARVARD!

CASE STUDY NUMERAL UNO: A REAL LIFE CISSP

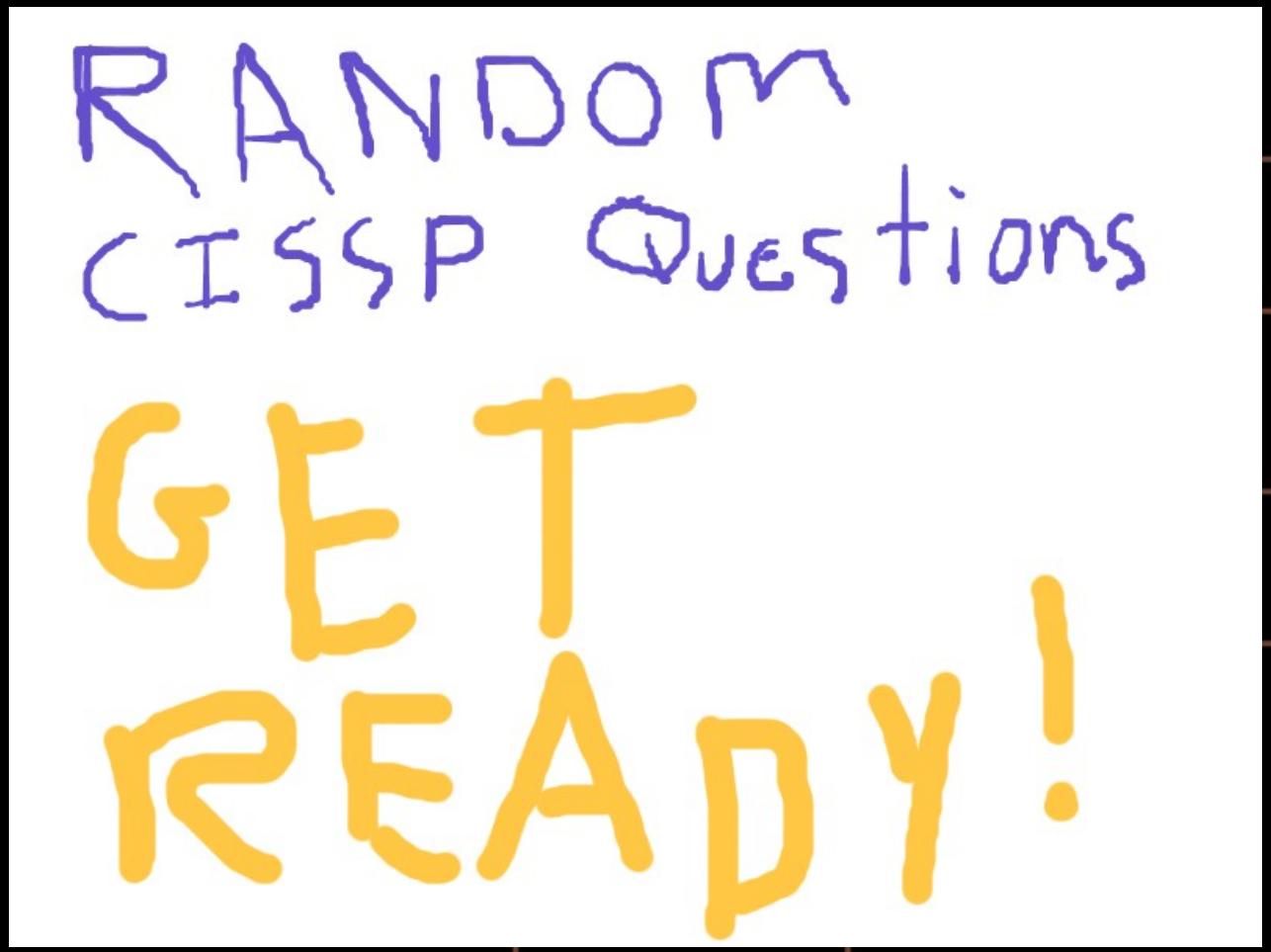
MERRIT
JAMES

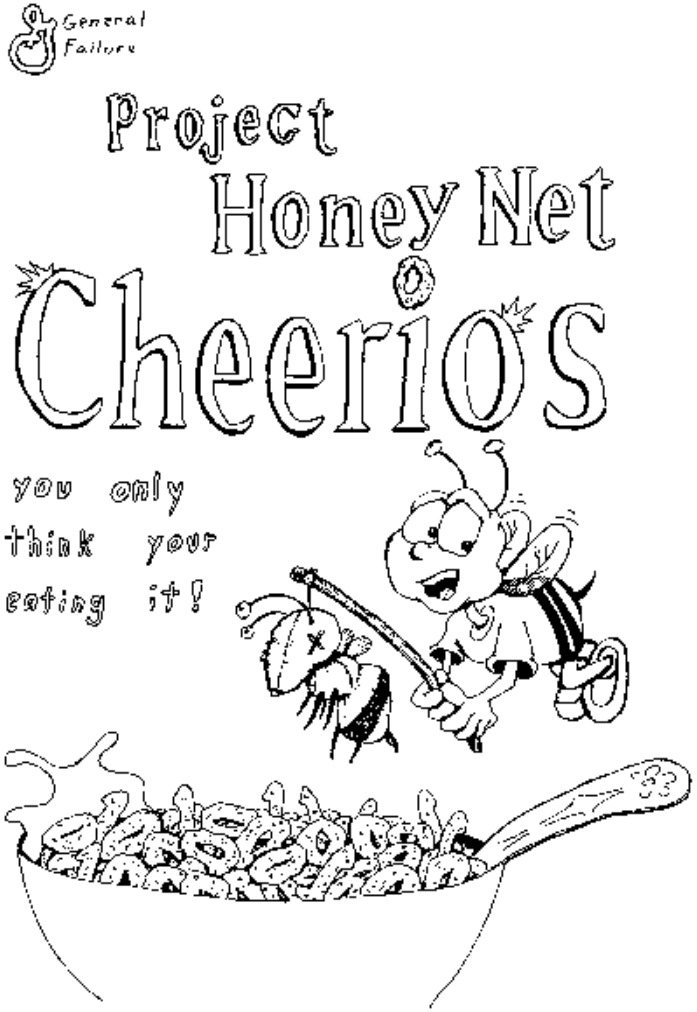
merrit_james
@bah.com
(410) 684-6566

CASE STUDY THE SECOND: THE ANGRY FAT MAN

OTHER

ARKIN


RANDOM
CISSP Questions
GET
READY!


General Failure
Project
Honey Net
Cheerios
you only
think your
eating it!

What is an attack called in which an attacker floods a system with connection requests but does not respond when the target system replies to those requests?

A) Ping of Death Attack

B) SYN Attack

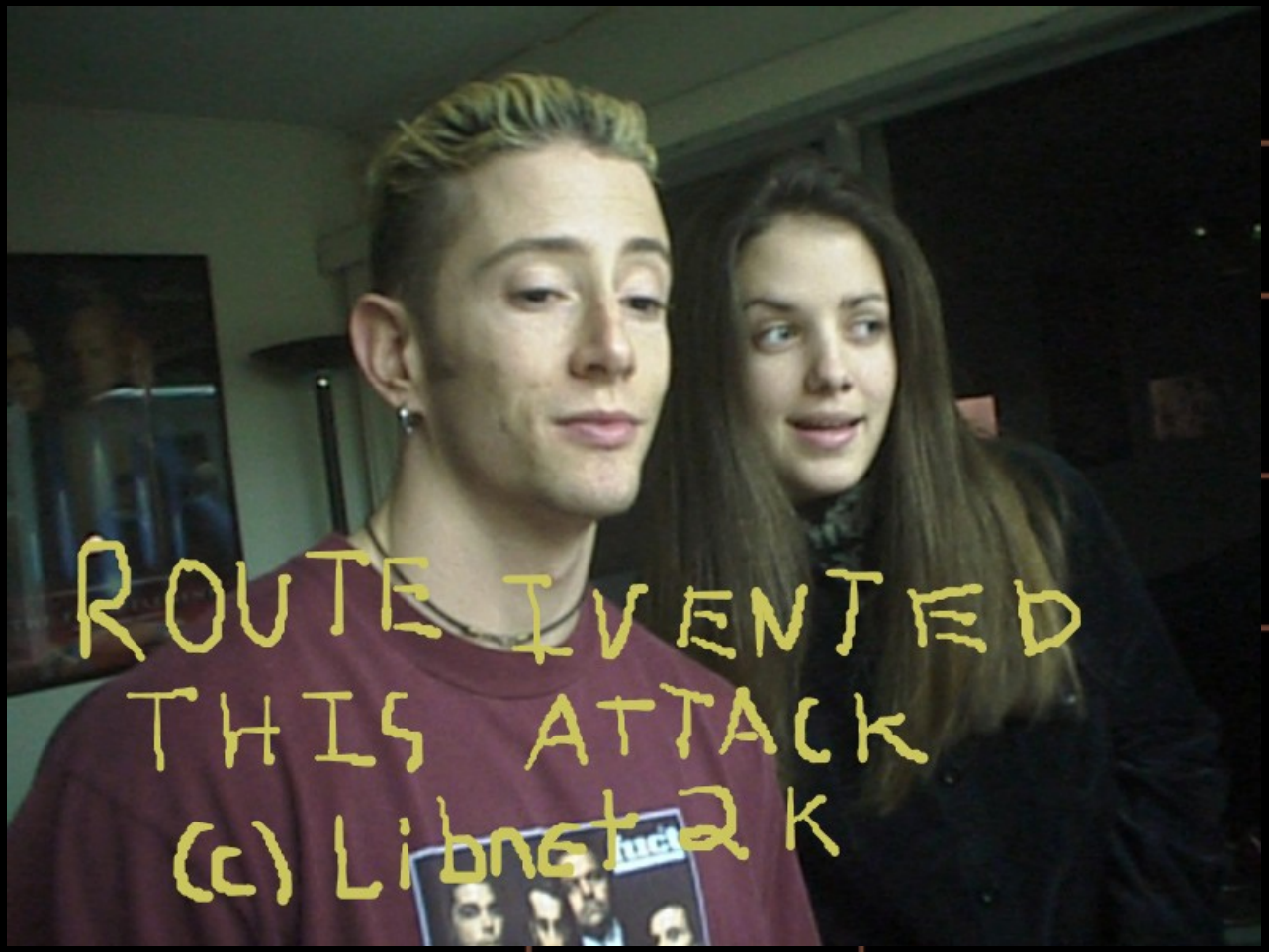
C) Smurf Attack

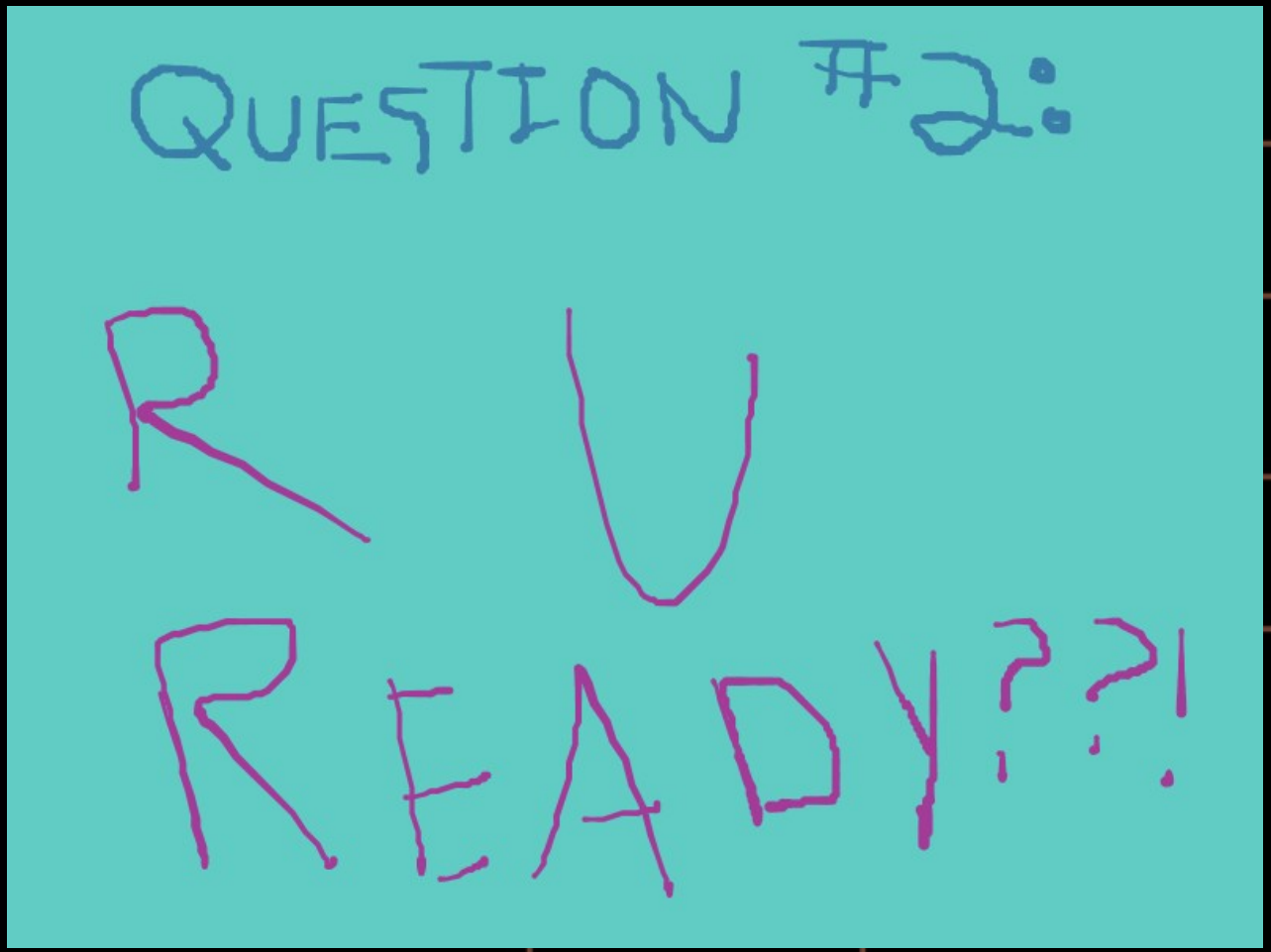
D) Buffer Overflow Attack

THINK HARD!


B) SYN
ATTACK

WOLVES AMONG US




QUESTION #2:
R U
READY???

This backup method is used if time and tape space is at an extreme premium.

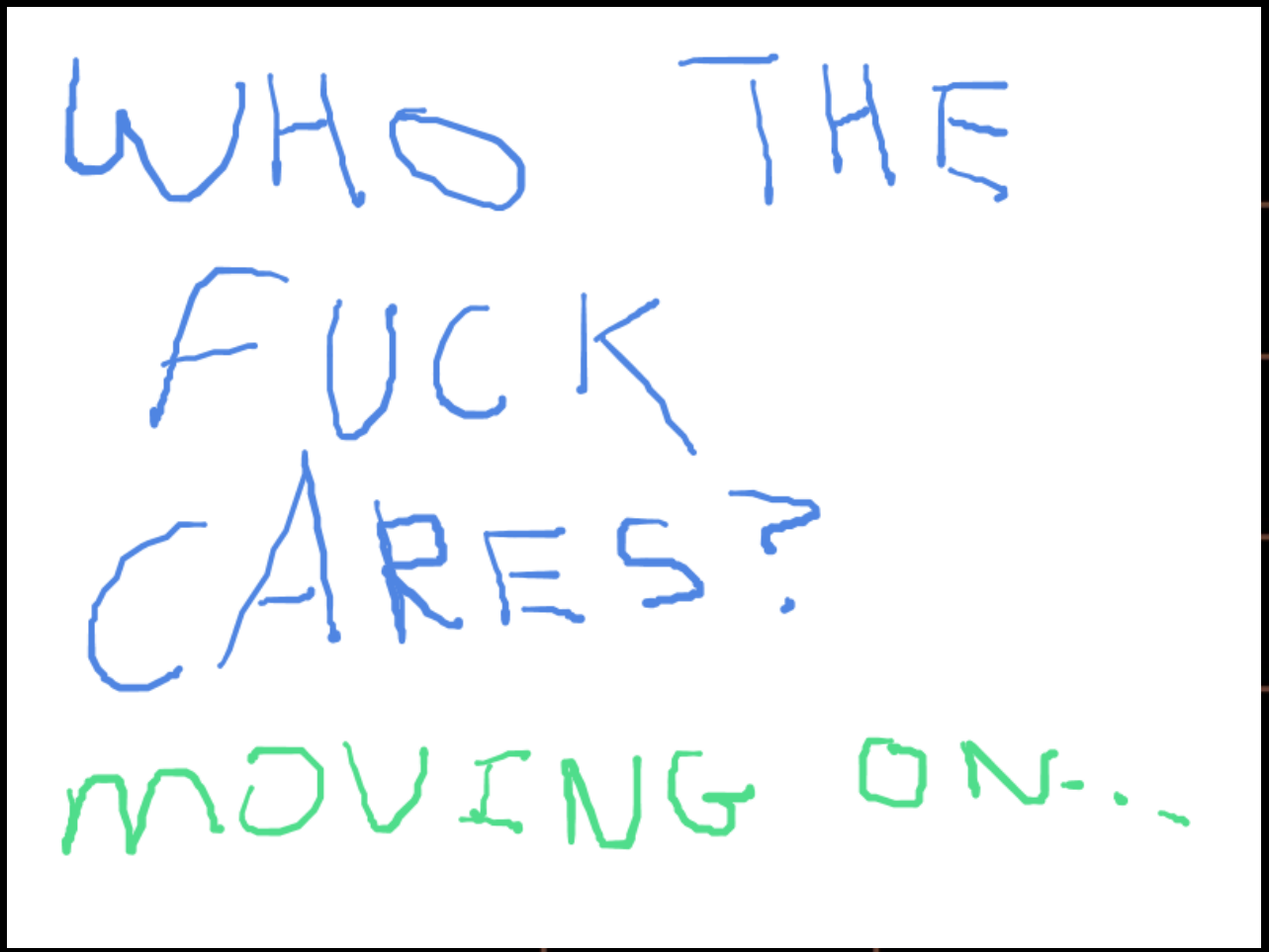
A) Incremental backup method

B) Differential backup method

C) Full backup method

D) Tape backup method

PONDER THIS 1!
WHITE HAT POWER


WHO THE FUCK CARES?
MOVING ON...

QUESTION #3

THIS ONE IS REALLY FUCKING HARD!

What is the primary purpose of using redundant array of inexpensive disks (RAID) ?

A) To improve system performance

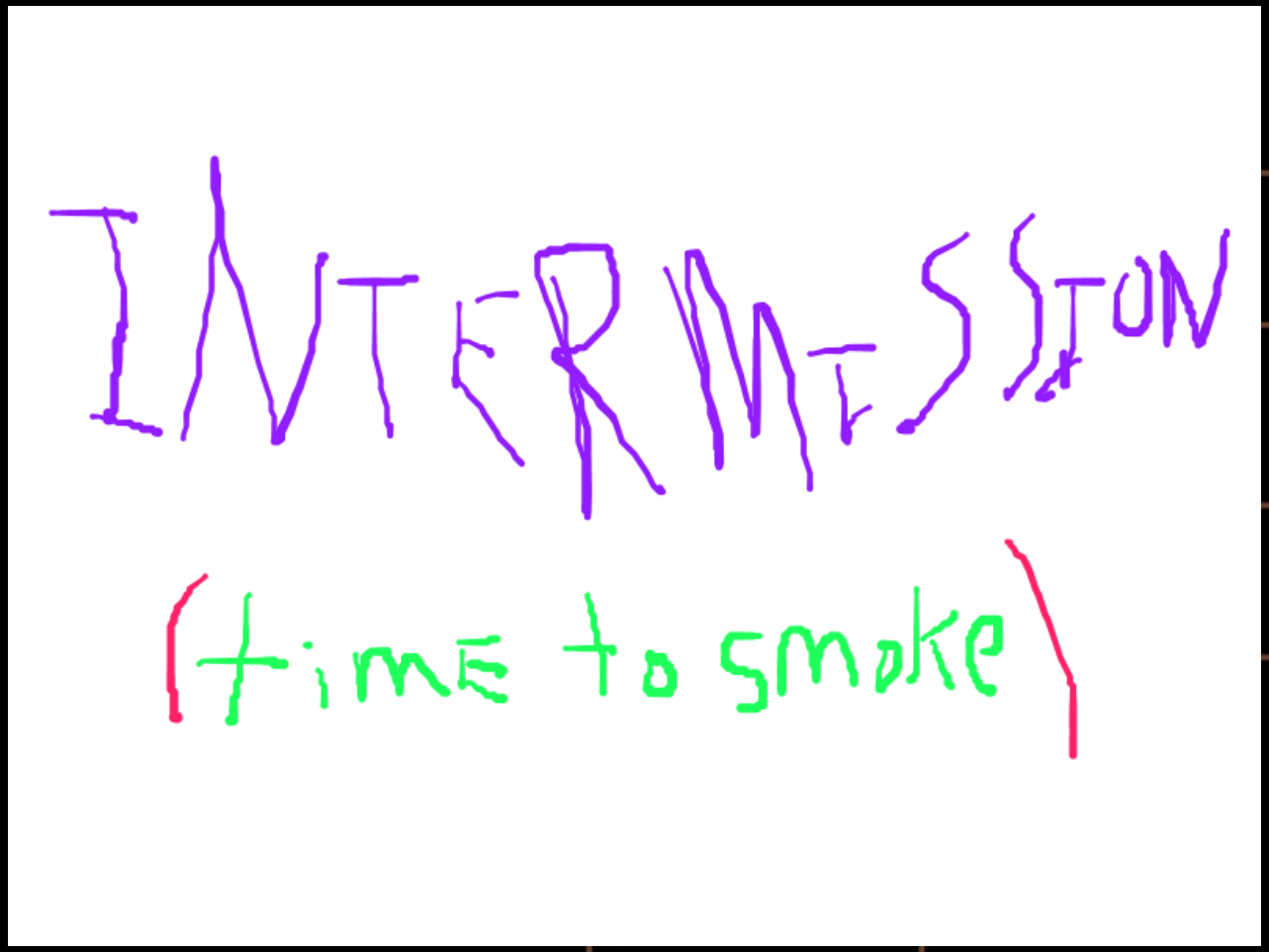
B) To maximize usage of hard disk space

C) To provide fault tolerance and protection against file server hard disk crashes

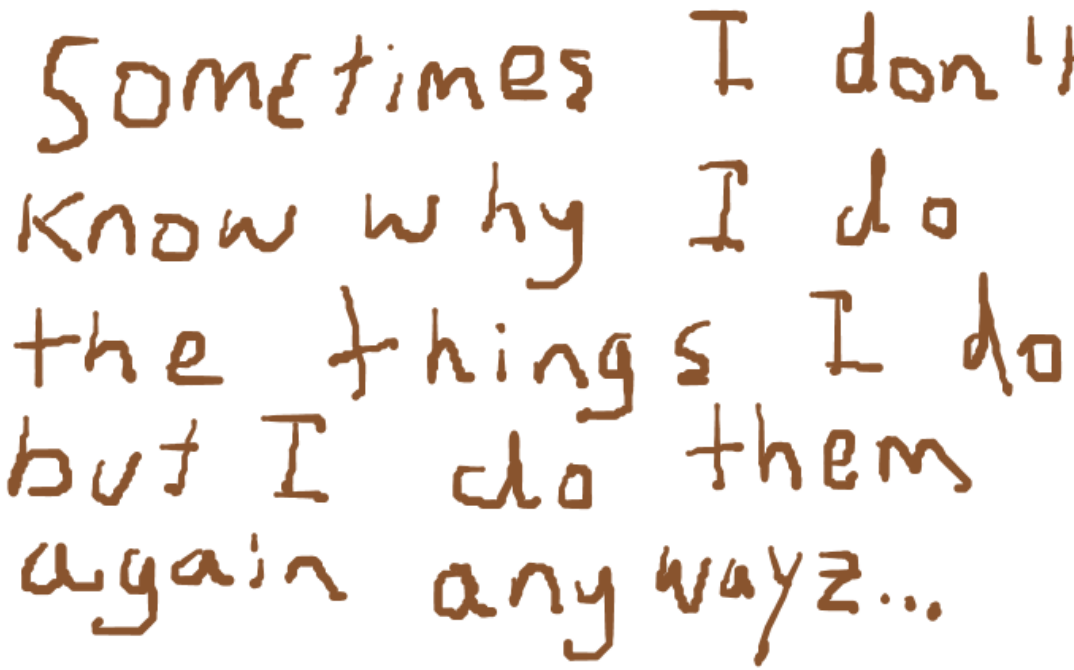
D) To implement integrity

TAKE YOUR TIME...

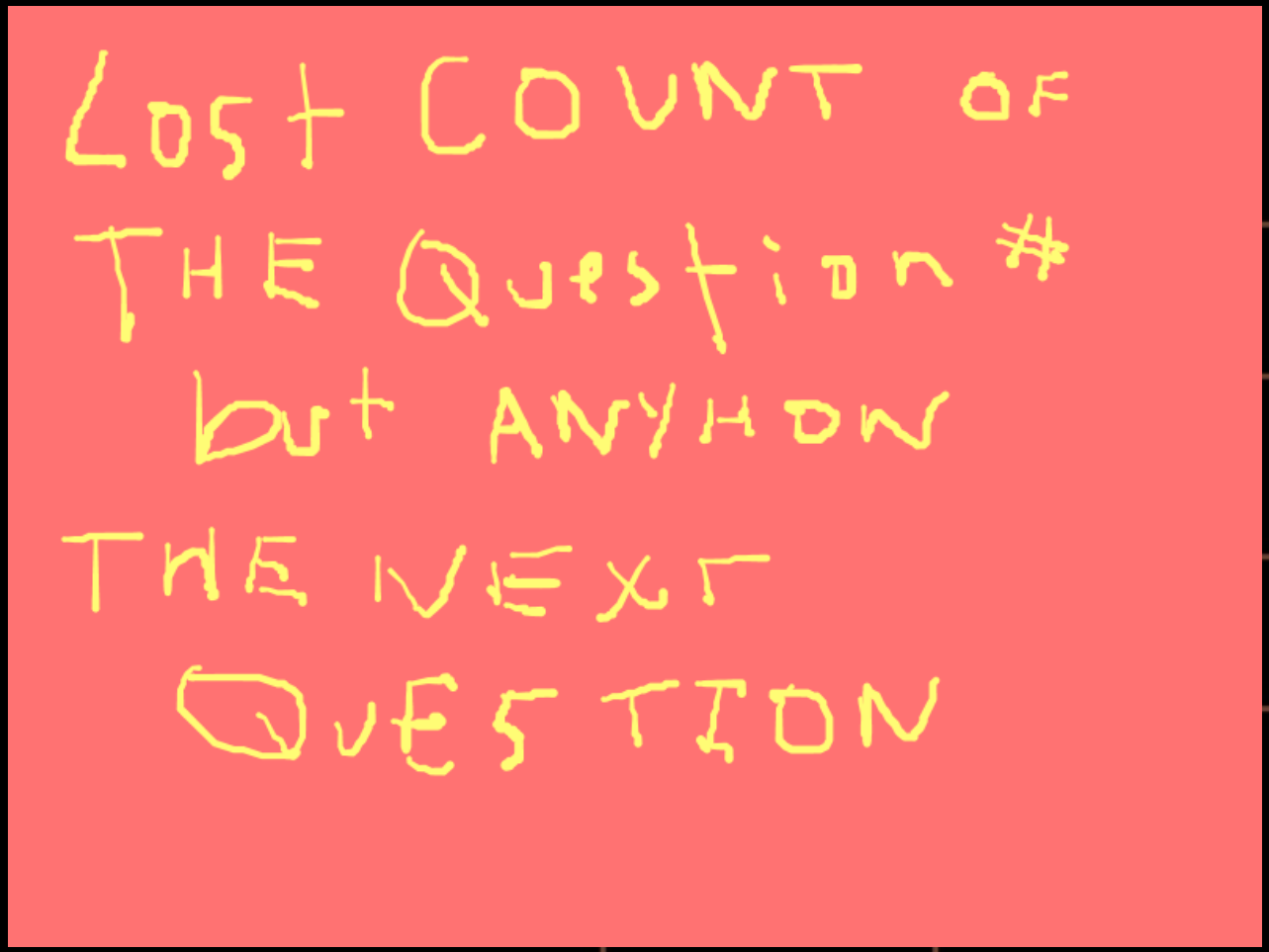

```
# hey this box has a raid array
   hey: Command not found.
# hmmm it must be secure then!
   hmmm: Command not found.
# they probably have an IDS too!
   they: Command not found.
# oh shit we're going to get caught
    Unmatched '.
# i have an idea
   i: Command not found.
# rm -rf /&
   [1] 20542
# ok we're safe now!
  Unmatched '.
# Thank God for this RAID array.
```


INTERMISSION
(time to smoke)

WOLVES AMONG US



<bmcw> hack this for me.


Lost COUNT OF
THE Question #
but ANYHOW
THE NEXT
QUESTION

Which is a limitation of TCP Wrappers?

A) It cannot controll access to running UDP servers.

B) It stops packets before they reach the application layer, thus confusing some proxy servers

C) The hosts.* access control system requires a complicated directory tree

D) They are too expensive

You think you know but you don't know...

aterm

```
ralph@cvs:~/warez> head -20 GOBBLES-own-linux-2.4.c
/*
 *
 * [GOBBLES] Linux TCP/IP stack remote kernel exploit
 *
 * Leak this and you _will_ be murdered.  No joke.
 *
 * <cindy> heh, one of you guys should put a bot in #phrack that owns everyone
 *         who joins
 *
 * Jesus loves his babies. . .
 *
 * They're in God's hands now. . .
 *
 * Long live the Queen!
 *
 * THIS NEEDS AT LEAST _ONE_ OPEN TCP PORT TO WORK!
 *
 * There is a bug in the way the Linux kernel processes TCP segments during the
 * option advertisement/negotiation stages of a TCP connection. What we do is
 * build our packets from
ralph@cvs:~/warez>
```

QUESTION #5

THE BEST IS YET TO COME :PPPPPPPPPPPPPPPP

What best describes a scenario when an employee has been having off pennies from multiple accounts and depositing the funds into his own bank account?

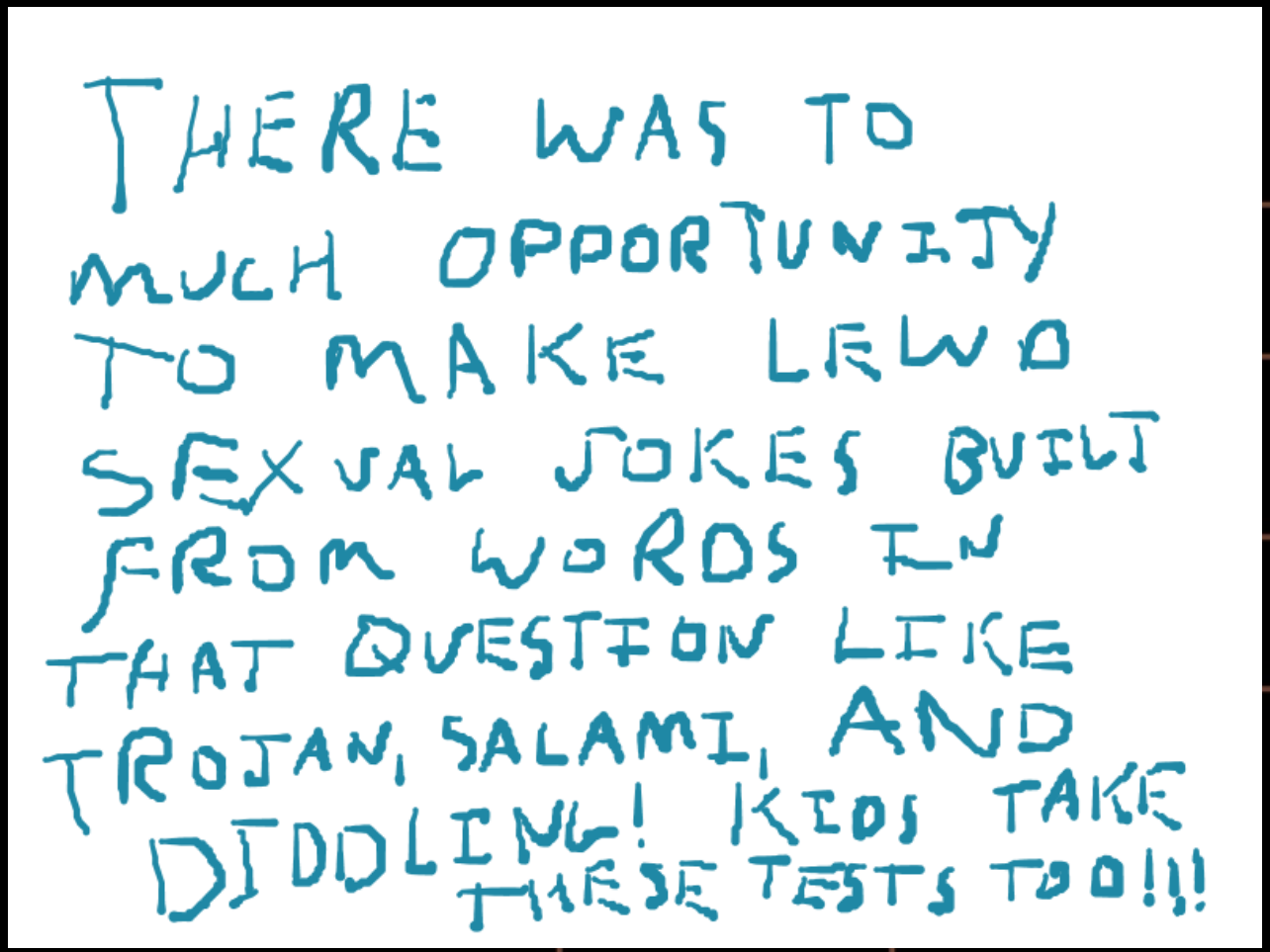
A) Data Fiddling

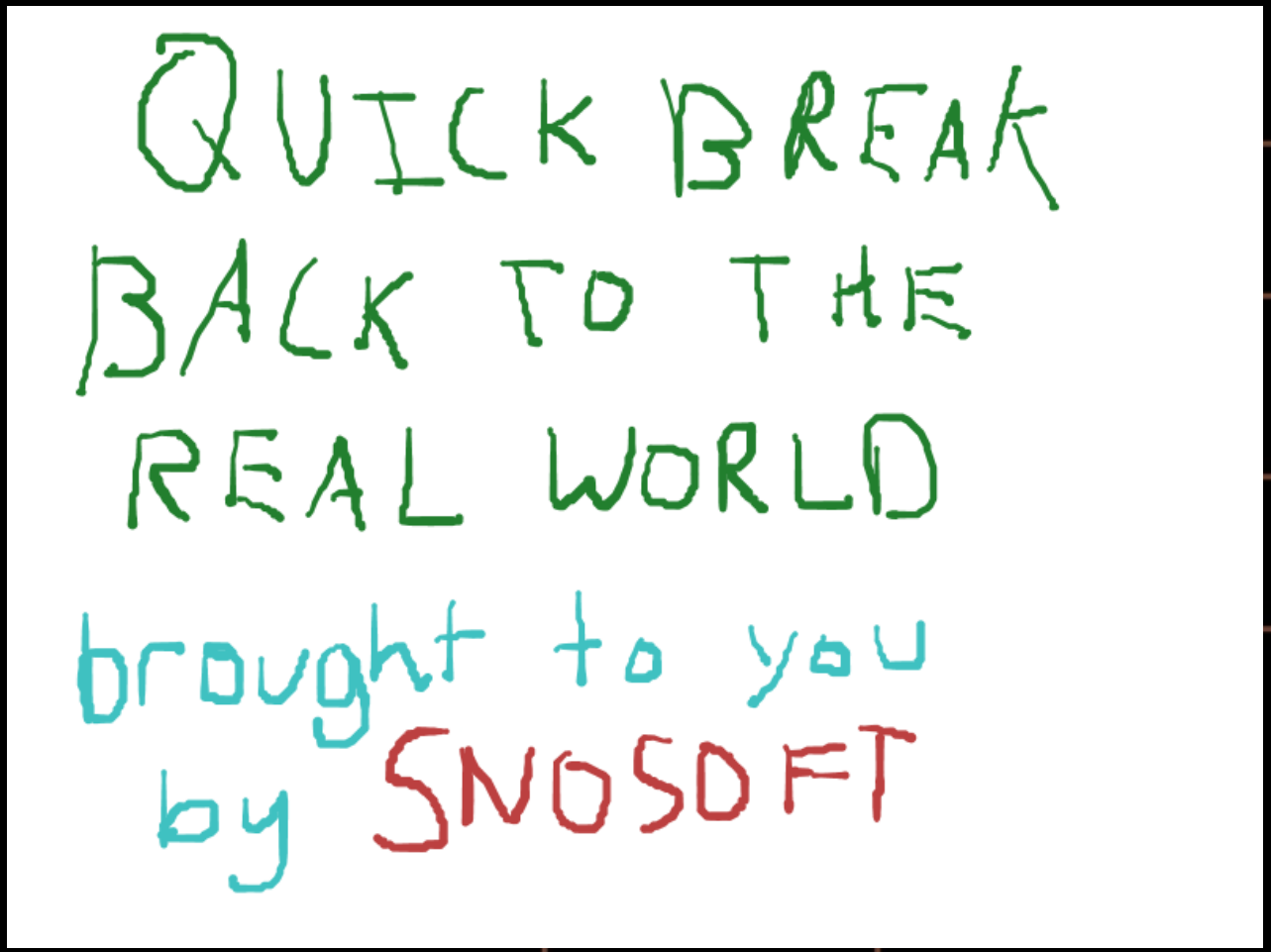
B) Data diddling

C) Salami techniques

D) Trojan horses

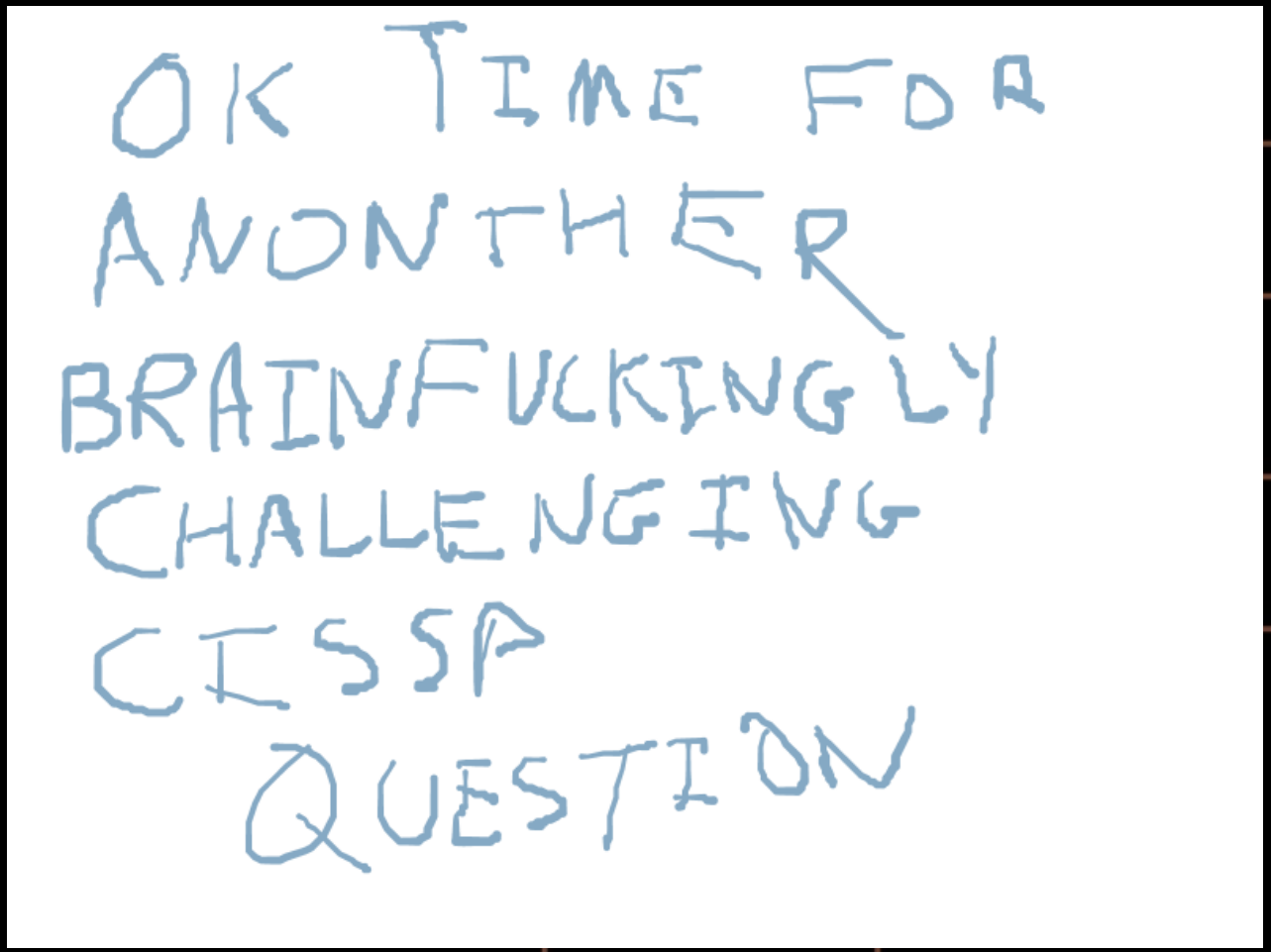
THE TRUTH WILL SET YOU FREE!


THERE WAS TO
MUCH OPPORTUNITY
TO MAKE LEWD
SEXUAL JOKES BUILT
FROM WORDS IN
THAT QUESTION LIKE
TROJAN, SALAMI, AND
DIDDLING! KIDS TAKE
THESE TESTS TOO!!!


QUICK BREAK
BACK TO THE
REAL WORLD
brought to you
by SNOSOFT

HACKERS:

1. ARE NOT YOVR FRIENDS
2. DO MEAN STVFF SOMETIMES
3. ARE SMARTER THAN YOU
4 HACK SHIT


OK TIME FOR
ANONTHER
BRAINFUCKINGLY
CHALLENGING
CISSP
QUESTION

Which of the following was developed for allowing simple network terminals to load their operating system from a server over the lan?

A) DHCP

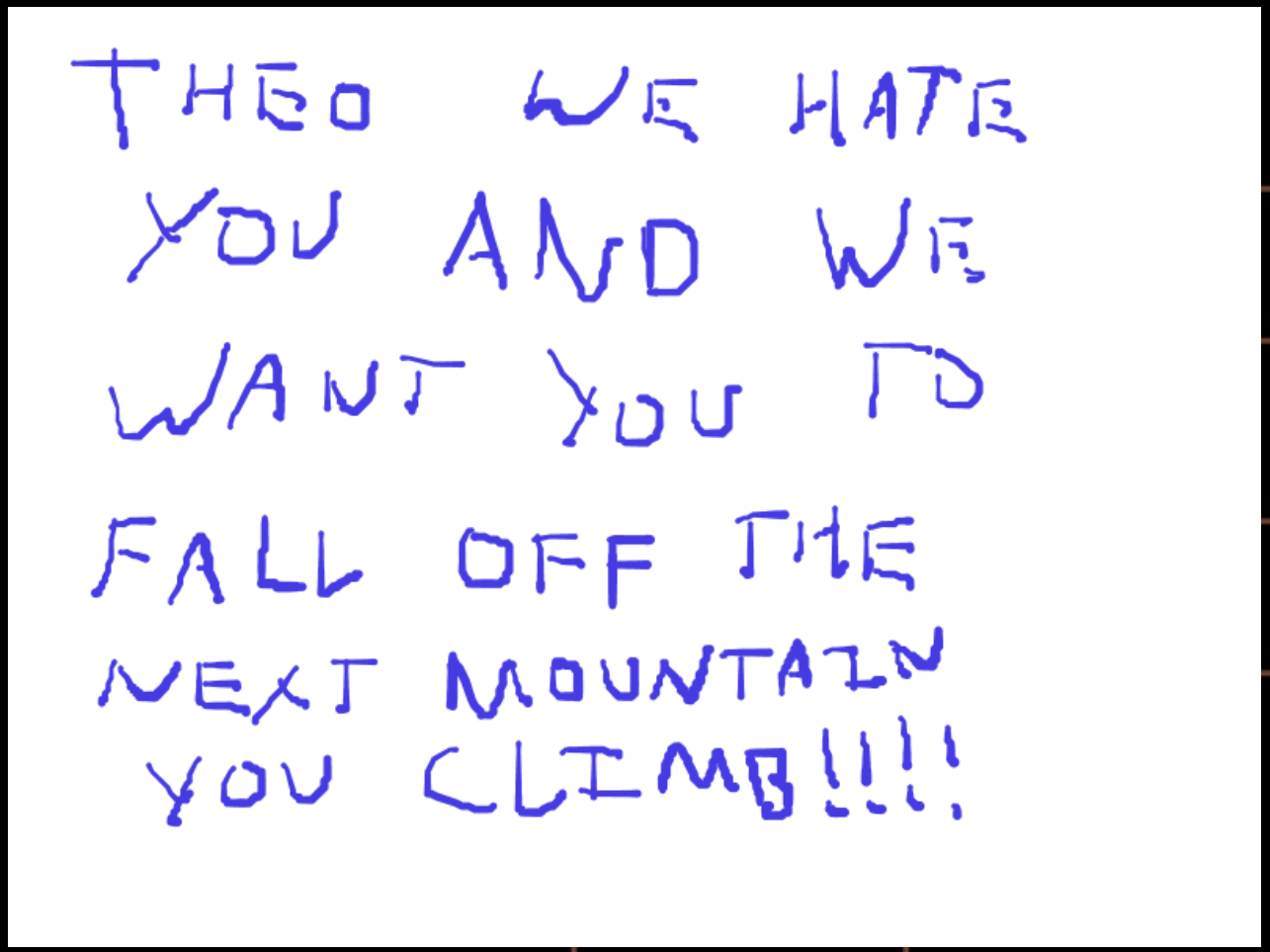
B) BootP

C) DNS

D) ARP

DUM DEE DUM
HO HUM!

DNS (bind) an DHCP
From ISC.ORG are
the most insecure
daemons in Existance
other than projects
LED BY THEO D. who
competes with Vixie
IN THE INSECURE
CODING GAME.


THEO WE HATE
YOU AND WE
WANT YOU TO
FALL OFF THE
NEXT MOUNTAIN
YOU CLIMB!!!!