“Fig Leaf Security”

@haroonmeer - 2011
Who am i ?

&

Why this talk?
A chance to meet our heroes!
like Simple Nomad!
"Decryption" of RCONSOLE Password

19981006: If an intruder recovers the encrypted password used during the loading of RCONSOLE, an attacker can use the recovered password to authenticate as the system owner and assume control of the system.

Lame NT Token Ring DoS

19980930: If you have Token Ring packets with bad data in them, you can crash NT from Microsoft (ask them for it, it's not on their FTP site).

GroupWise Buffer Overflow

19980923: You can overflow the POP3 and LDAP ports causing the server to crash. Account names is bad, but crashing servers is good. At least with the latest patches of GroupWise, Novell has released a patch, look for gwia551.exe at support.novell.com. The patch is designed to improve the security of the GroupWise server and prevent buffer overflows.

Default NDS Rights
thegnome: we expected
thegnome: we got
this is my rant..
• The infosec industry
• ZA infosec research
InfoSec: We Suck
and it’s our fault
No ?
Bet on your architecture?
Write code for a living?
So we build secure networks, but can’t protect our most prized user and we write code, that we know can’t stand up to security testing?
but nobody can write secure code
Right?
Wrong!
<Brief Digression>
(sub-rant)
Do you know these men?
we hero worship the wrong guys..
</Brief Digression>

(sub-rant)
but nobody can write secure code
ok. not

(secure and usable)
Really?
sendmail vs qmail ?
djbdns vs bind ?
So why did we think otherwise?
Charlatans
fig leaves!
Application Testing..
“Halting Problem!”
“patching is a hard” problem
Management don't buy in!
AV's and V's
Why the double standard?
We (seem to) only fight the fights we can (kinda) win
aka: “buying what ppl are selling”
hiding behind our fig leaves..
“You & Your Research”

http://www.cs.virgina.edu/~robins/YouAndYourResearch.html
So why don’t we do more?
it’s hard..
easy to start..
(ideas are cheap)
Research Fig Leaves
XXX is lame
Academic masturbation!
“doesn’t impress me”
Distraction

Aldous Huxley vs. George Orwell
Author: "Brave New World"  Author: "Nineteen Eighty-Four"
WHAT HUXLEY FEARED WAS THAT THERE WOULD BE NO REASON TO BAN A BOOK, FOR THERE WOULD BE NO ONE WHO WOULD WANT TO READ ONE.

"THE BIGGEST LOSER" WILL BE BACK AFTER THESE MESSAGES...
Huxley feared those who would give us so much that we would be reduced to passivity and egotism.
“Amusing ourselves to Death”
Michael Howard

Average Blog Posts per Month (before twitter) | 5.9
Average Blog Posts per Month (after twitter) | 1.7
Average Tweets per Month | 77.5
Net result of twitter-effect | -71%

http://twitter.com/michael_howard
http://blogs.msdn.com/michael_howard
No Interesting Problems..
“Work on stuff that matters”

“New Threats to Privacy”
There are important battles to fight..
“Don’t just be the guy who tweeted about it”
Don’t just fight the fights we can (kinda)win
Fight the fights that need fighting
We need to produce more than we consume..
We need you

haroon@thinkst.com
@haroonmeer