



indonesian
security
conference
2008



Social Engineering :

the art of 'hacking'

K-159

k-159@echo.or.id





Agenda

- Introduction [self & e-rdc]
- Prolog [true story, the artist]
- Social Engineering [Def, Goal, Type, Impact]
- Defence from Social Engineering
- Demo / Q & A

Introduction

Self & e-Rdc

Self

- Handle : K-159, its Russian Nuclear Submarine
- Realname : M.Hasran Addahroni
- web : <http://k-159.echo.or.id>
- Status : Married, 2 children
- Education : SI Electrical Engineering
- Occupation : Senior Security Analyst

PT.SCAN-Nusantara



www.scan-nusantara.net

- Achievements : Runner Up PANHAC BALI 2006
- Publication : Released more than 40 advisories with ECHO and published in security mailing-list bugtraq@securityfocus.com, milw0rm.com, etc

ECHO

- IndonEsian Community for Hackers and Open Source
- The stressing is still around the hacking stuffs. We're working on the Open Source activities
- Ezines, Advisories, News, Forum, Mailing list
- Founded in 2003
- Has **13** staff a.k.a ECHO STAFF
- Has **11116** mailing lists member, and **14151** Board Discussions member (Jan,22 2008)
- <http://echo.or.id> || <http://e-rdc.org>



Prolog

true story, the artist



**indonesian
security
conference
2008**



There is no patch to human stupidity..



**indonesian
security
conference
2008**



ECHO.or.id



Kevin Mitnick

Name: Kevin Mitnick

Handle(s): Condor, from the movie
Three Days of the Condor

Age: 40

Place of birth: California, USA

Marital status: Divorced. Now lives with girlfriend
and her eight year-old daughter

Current residence: Las Vegas, USA

Job: Chief executive of Defensive Thinking

First computer: Toshiba 4400 SX laptop

Best known for: His notoriety

Area(s) of expertise: Social engineering





the Badir brothers



indonesian
security
conference
2008



Name: Muzher,Shadde,Ramy Badir

Age: 28,22,27

Place of birth:Kafr kassem,Midle East

Condition:has been blind since birth

Programing Language : C, C++, Basic, Java,
HTML, PHP, CGI

Area(s) of expertise: Social engineering/phreaking



Social Engineering

Definition,type,goal,impact



navigasi

- [Halaman Utama](#)
- [Perubahan terbaru](#)
- [Peristiwa terkini](#)
- [Halaman sembarang](#)

pencarian

komunitas

- [Warung Kopi](#)
- [Portal komunitas](#)
- [Bantuan](#)

wikipedia

- [Perihal Wikipedia](#)
- [Pancapilar](#)
- [Kebijakan](#)
- [Menyumbang](#)

kotak peralatan

- [Pranala balik](#)

[halaman](#) [pembicaraan](#) [sunting](#) [↑](#) [versi terdahulu](#)

Dukung Wikipedia: sebuah proyek nirlaba.

[Menyumbang »](#)

[\[Tampilkan\]](#)

Social engineering (keamanan)

Dari Wikipedia bahasa Indonesia, ensiklopedia bebas

Social engineering adalah pemerolehan **informasi** atau maklumat rahasia/sensitif dengan cara menipu pemilik informasi tersebut. *Social engineering* umumnya dilakukan melalui **telepon** atau **Internet**. Social engineering merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu.

Social engineering mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Seperti kita tahu, tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung platform, sistem operasi, protokol, **software** ataupun **hardware**. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap orang yang mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan kamanan yang telah disusun. Seperti metoda hacking yang lain, social engineering juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri.

Faktor utama

[\[sunting\]](#)

Di balik semua sistem keaman dan prosedur-prosedur pengamanan yang ada masih terdapat faktor lain yang sangat penting, yaitu : manusia.

Pada banyak referensi, faktor manusia dinilai sebagai rantai paling lemah dalam sebuah sistem keamanan. Sebuah sistem keamanan yang baik, akan menjadi tidak berguna jika ditangani oleh administrator yang kurang kompeten. Selain itu, biasanya pada sebuah jaingan yang cukup kompleks terdapat banyak user yang kurang mengerti masalah keamanan atau tidak cukup peduli tentang hal itu. Ambil contoh di sebuah perusahaan, seorang network admin sudah menerapkan kebijakan keamanan dengan baik, namun ada user yang mengabaikan masalah kamanan itu. Misalnya user tersebut menggunakan password yang mudah ditebak, lupa logout ketika pulang kerja, atau dengan



Gaining Human Nature

- trust
- fear
- desire to help



Social Engineer Goal

- sensitive information
- authorization details
- access details



Social Engineer Common Target

- Customer Services and Help desk
- Technical Support
- Vendor
- System Administrator and User

Type of Social Engineering

- **Human-based :**

refers person to person interaction to retrieve desire informations

eq:dumpsterdiving,tailgating,piggybacking,eavesdropping,shoulder surfing,reverse social engineering.

- **Computer-based :**

having computer software that attempts to desire informations

eq:pop up windows,phising,hoax & chain letters

Human-based Social Engineering behaviour

- Legitimate end user :

gives identity and ask for sensitive information.

- Important user:

posing as VIP of a target company, valuable customer.

Dumpster Diving

- **search for sensitive information :**
trash-bins,printer-trash bins,user desk for sticky notes.
- **collect:**
phone bill,contact information,financial information,etc



Tailgating

- un authorized person using a fake ID following authorized person, enter secured areas



Piggybacking

- “i forgot my ID card,please help”
- authorized person give access to un authorized person by keeping the secure door open

Shoulder Surfing

- looking over shoulders to get information such as passwords as you enter password
- simply by looking over shoulders or use binocular.

Phishing

- fake email to user to give access user detail
- the statement such as : verify your account,update your user information,.



Anatomy of Attack

- Research Target [dumpster diving, website, employee, etc]
- Selected Victim [identify of frustrated employee]
- Develop Relationship
- Exploit Relationship [collect sensitive account info, financial info, current technologies]



Social Engineering Impact

- website defacement/systems compromised
- economic loses (revenue,brand,trust,recovery)
- data stolen
(account,privacy,cc,employee,student,gov,artis)

Defence

protect your self,property,company



indonesian
security
conference
2008



it is much easier to trick someone into giving a password for a system than to spend the effort to hack into the system

[Kevin Mitnick]

How to defence

- training to increase security awareness
- password policies : periodic password change, avoid default password, account blocking after failed attempts, length & complecity password
- operational guidelines : ensure security of sensitive information and authorized use of resources



How to defence (cont)

- classification of information as top secret, for internal use only, for public use only, etc
- access privileges : admin, user, guest with proper authorization
- background check of employees
- physical security policies [ID card, uniform, security personnel etc]



indonesian
security
conference
2008



References

- wikipedia.org
- wired.com, zdnet.com.au,
- EC - Council CEH module
- securityfocus.com
- others



indonesian
security
conference
2008



Thanks to

- Teknik Informatika UPN [v] Jogja
- Comitee idsecconf.org
- Depkominfo
- PT.SCAN Nusantara www.scan-nusantara.net
- Cipta Karya www.ciptakarya.co.id

Epilog

Q & A