

Urusetia Keselamatan ICT Negeri



Pengodam : Teknik
Serangan dan
Bagaimana Mencegah.

07 Julai 2009
Seminar Wilayah ICT
Jabatan Perkhidmatan Komputer Negeri

Presentation Outline

- ⊙ Objektif
- ⊙ Introduction
- ⊙ What is Hacking?
- ⊙ Hacker Classes.
- ⊙ Can Hacking be Ethical?
- ⊙ Hacking Cycle

Presentation Outline

- ① 1st Step : Reconnaissance.
- ② 2nd Step : Scanning.
- ③ 3rd Step : Gaining Access.
- ④ 4th Step : Maintaining Access.
- ⑤ 5th Step : Covering or Clearing Tracks
- ⑥ Type of Hacking
- ⑦ What Happen Today?
- ⑧ Conclusion



Objective

Objektive

- ⊙ Memberi pendedahan kepada peserta tentang apakah *hacker* yang beretika.
- ⊙ Memberi penerangan lanjut mengenai kitaran kerja sesuatu pencerobohan berlaku.
- ⊙ Berkongsi cara-cara atau kaedah-kaedah untuk meminimumkan aktiviti pencerobohan dari berlaku.
- ⊙ Mengenalpasti sumber-sumber yang sering digunakan oleh penceroboh untuk memasuki sesuatu sistem.
- ⊙ Menjelaskan langkah-langkah yang perlu diambil bagi menghalang dari berlakunya pencerobohan pada komputer/server masing-masing.



Introduction

Introduction

- ⦿ Kursus EC-Council Certified Ethical Hacking(CEH) mengajar peserta mengenai bagaimana penceroboh melakukan aktiviti jahatnya.
- ⦿ Kursus ini memberi pendedahan bagaimana pencerobohan dilakukan oleh penceroboh seperti SQL injection, Denial of Service, Social Engineering, Password Cracking, Session Hijacking dan sebagainya terhadap sesuatu sistem.
- ⦿ Melalui kursus ini, ia memberi maklumat awal apakah pertahanan yang diperlukan/dilaksanakan dari perspektif pencerobohan agar masa dapat dijimatkan dalam mempertahankan sesuatu sistem.



What Is Hacking?

What is Hacking?



What is Hacking?

- ⦿ Menurut www.dictionary.com, hacking membawa maksud : To use one's skill in computer programming to gain illegal or unauthorized access to a file or network.

Hacker Class

- ⦿ Black Hats
- ⦿ White Hats
- ⦿ Gray Hats
- ⦿ Suicide Hackers

Ethical Hacker Class

- ⊙ Former Black Hats
- ⊙ White Hats
- ⊙ Consulting Firms



Can Hacking be
Ethical?

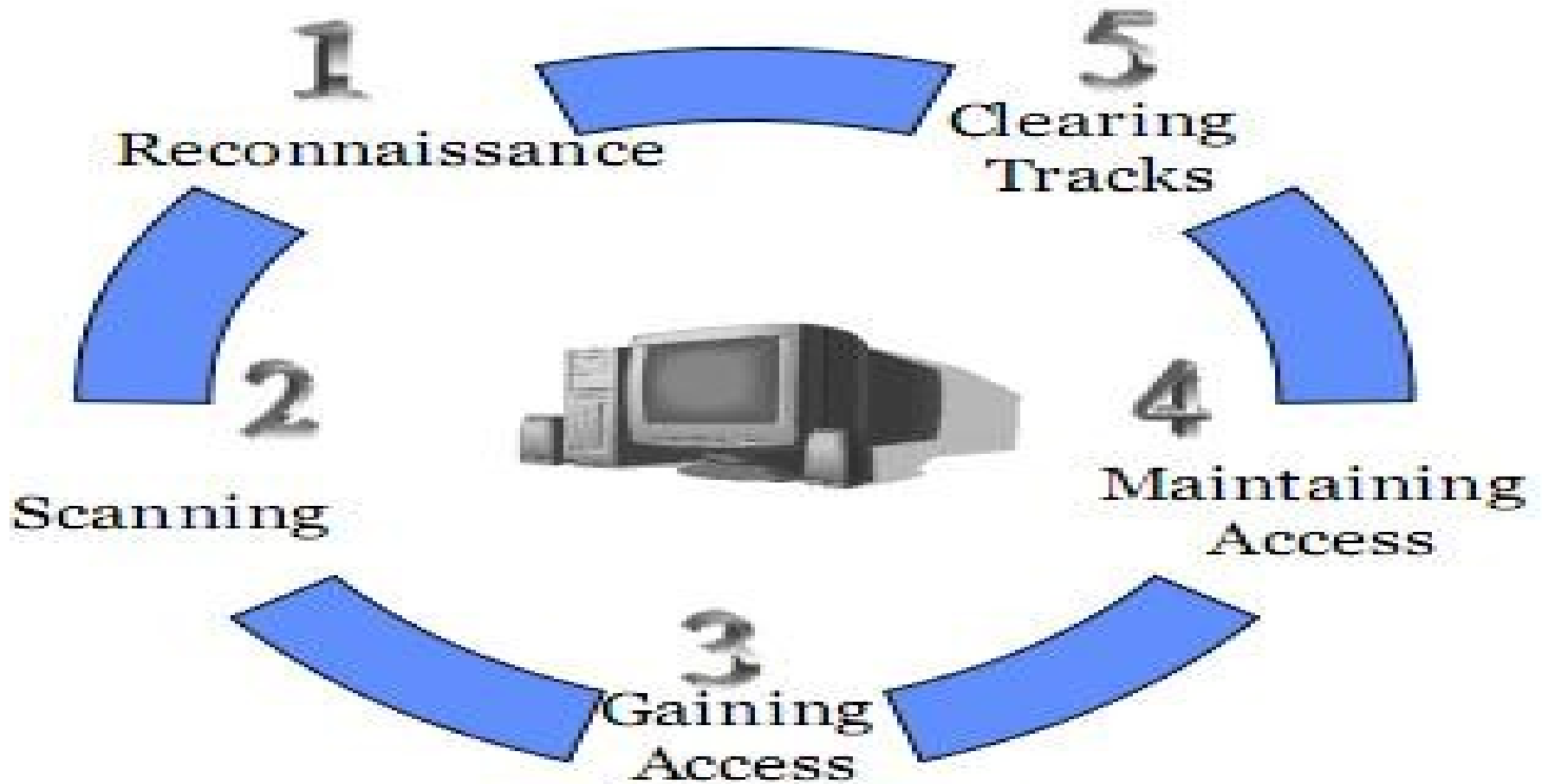
Can Hacking be Ethical?

- ⊙ Menurut EC-Council berikut adalah takrifan mereka mengenai Hacker, Cracker, Hacking dan Ethical Hacker.
- ⊙ **Hacker** : Individu yang gembira untuk belajar dan mengetahui komputer secara terperinci.
- ⊙ **Cracker** : Individu yang menggunakan pengetahuannya untuk tujuan jahat.
- ⊙ **Hacking** : merujuk kepada kepesatan pembangunan program-program komputer yang baru atau reverse engineering terhadap program komputer sedia ada bagi menjadikan program komputer tersebut lebih baik dan efisien.
- ⊙ **Ethical hacker** : Merujuk kepada individu keselamatan yang menggunakan pengetahuan komputer untuk tujuan kebaikan.



Hacking Cycling

Hacking Cycle





Reconnaissance

Reconnaissance

- ⊙ Proses awal pengumpulan maklumat terhadap sistem yang akan diuji.
- ⊙ Juga dikenali dengan nama “Footprinting”.
- ⊙ Dikenali dengan panggilan “rattling the door knobs”, bermaksud untuk melihat jika ada sebarang tindakbalas daripada pemilik sistem.

Reconnaissance - Countermeasure

- ⊙ Pastikan semua maklumat rasmi dan sulit di *shred* sebelum dibuang.
- ⊙ Pastikan individu yang masuk ke dalam pejabat adalah mereka yang sah sahaja.
- ⊙ Jangan dedahkan maklumat perkomputeran pejabat anda kepada orang yang tidak dikenali secara sah.



Scanning

Scanning

- ⦿ Langkah awal pengujian atau serangan terhadap sesuatu sistem.
- ⦿ Ia merupakan proses untuk mengenalpasti ruang untuk memasuki sesuatu sistem.

Scanning

- ⊙ Mengenalpasti sistem yang aktif di dalam rangkaian.
- ⊙ Mencari port yang aktif dan sedang berfungsi.
- ⊙ Mengenalpasti jenis OS komputer yang ingin diceroboh.
- ⊙ Mengenalpasti services yang sedang berfungsi pada komputer yang ingin dicerobohi.
- ⊙ Mengenalpasti IP komputer yang ingin dicerobohi.

Scanning – Countermeasures

- ⊙ Use FIREWALL
- ⊙ Use Network Intrusion Detection System and Network Intrusion Prevention System.
- ⊙ Any sensitive information should not be disclosed publicly over the Internet.



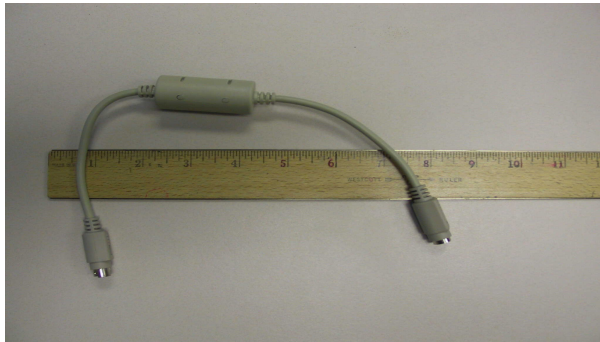
Gaining Access

Gaining Access

- ① Merujuk kepada fasa penceroboh berjaya memasuki sesuatu sistem.

Classification. Hardware keyloggers

⊙ KeyGhost keylogger



⊙ KeyKatcher keylogger



Keyboard cable with KeyGhost installed



Keyboard cable with KeyKatcher installed



Password Cracking - Countermeasures

- ⦿ Enforce 8-12 character alphanumeric passwords. Please refer to SGCert, http://www.sgcert.org/policies/Password_Policy.pdf
- ⦿ Set the policy change policy to 30 days
- ⦿ Physically isolate and protect the server
- ⦿ Monitor the server logs for brute force attacks on user account
- ⦿ NEVER give password to other people.
- ⦿ NEVER stick your password on the computer screen, cubical or drawer.

Executing – Countermeasures

- ⊙ Don't DOWNLOAD BLINDLY from people or site that you are not 100% sure about.
- ⊙ Even you get the file from friend, confirm with friend before open the file attach.
- ⊙ Dont use any features in email programs that automatically get or preview files.
- ⊙ Don't click any addresses link inside your email until you sure about it.
- ⊙ Update your antimalware regularly.
- ⊙ Use personnal firewall.



Maintaining Access

Maintaining Access

- ⦿ Mengekalkan pencerobohan dari dikesan untuk kegunaan segera atau kemudian hari.



Maintaining Access - Rootkit

Countermeasures - Rootkits

- ⦿ Back up critical data and reinstall OS/application from a trusted source.
- ⦿ Do not rely on backup, as there is a chance of restoring from Trojaned software.
- ⦿ Keep a well-documented automated installation procedure.
- ⦿ Store availability of trusted restoration media.
- ⦿ Regularly scan computer using anti-rootkit software from F-Secure, Sophos, Webroot or Microsoft..
- ⦿ Install software from their main source or trusted site.



Covering or Clearing Track

Covering or Clearing Track

- ① The Last step hacker do to hide his/her tracks.
- ① What his/her do?
 - 1) Disabling Auditing
 - 2) Clearing the Event Log

Contermeasures - Covering or Clearing Track

There is NO
COUNTERMEASURES as the
hacker already inside your system!
Except.....reformat your computer/
server.....☹



What Happen
Today?

“The Biggest Military Computer Hack of all Time”

Gary McKinnon, a systems administrator gained illegal access and made unauthorized modifications to 97 computers belonging to the US government, including computers from the DoD, NASA and the National Security Agency over 12 months



The US government said McKinnon's hacking caused downtime and personnel costs of around \$1m (£0.6m)

Lethal Weapons -
software available
freely over the internet
were used to gain access to computer networks used by the US Army, Navy & Air Force

ShadowCrew

United States Secret Service

WWW.SECRETSERVICE.GOV



SHADOWCREW

"FOR THOSE WHO WISH TO PLAY IN THE SHADOWS....."



ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE

SEVERAL ARRESTS HAVE RECENTLY BEEN MADE...WITH MANY MORE TO FOLLOW.

Proxies, VPNs, IP Spoofing, Encryption, etc.... You Are No Longer Anonymous!!

Where do you want to go Today?

The Internet home of: **FORTUNE Money BUSINESS 2.0** FORTUNE SMALL BUSINESS [Subscribe to](#)

CNNMoney.com

GET QUOTES SYMBOL LOOK-UP **SEARCH** [Entire Site](#)

HOME NEWS MARKETS TECHNOLOGY JOBS & ECONOMY

News

40M credit cards hacked

Breach at third party payment processor affects 40 million MasterCards.

July 27, 2005: 6:16 PM EDT
By Jeanne Sahadi, CNN/Money senior writer

NEW YORK (CNN/Money) - Over 40 million card accounts were exposed to potential fraud due to a security breach that occurred at a third-party processor of payment card transactions, MasterCard International said last Friday.

"It looks like a hacker gained access to CardSystems' database and installed a script that acts like a virus, searching out certain types of card transaction data," said MasterCard spokeswoman Jessica Antle.

Of the cards involved, 13.9 million were MasterCard-branded cards, which include Maestro

CNN.com/TECHNOLOGY

SEARCH The Web CNN.com **Search**

- Home Page
- World
- U.S.
- Weather
- Business at CNNMoney
- Sports at SI.com
- Politics
- Law
- Technology**
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports

SERVICES

- Video
- E-mail Newsletters
- CNNtoGO

SEARCH

Web CNN.com

Search Powered by **YAHOO!** search

FTC: Identity theft strikes 1 in 8 adults

Report says thieves cost \$53 billion last year

By Jeordan Legon
CNN
Wednesday, October 29, 2003 Posted: 1:01 PM EST (1801 GMT)

(CNN) -- In the most comprehensive look to date at a fast-growing crime, the Federal Trade Commission said Wednesday nearly one in eight U.S. adults fell victim to identity theft in the last five years.

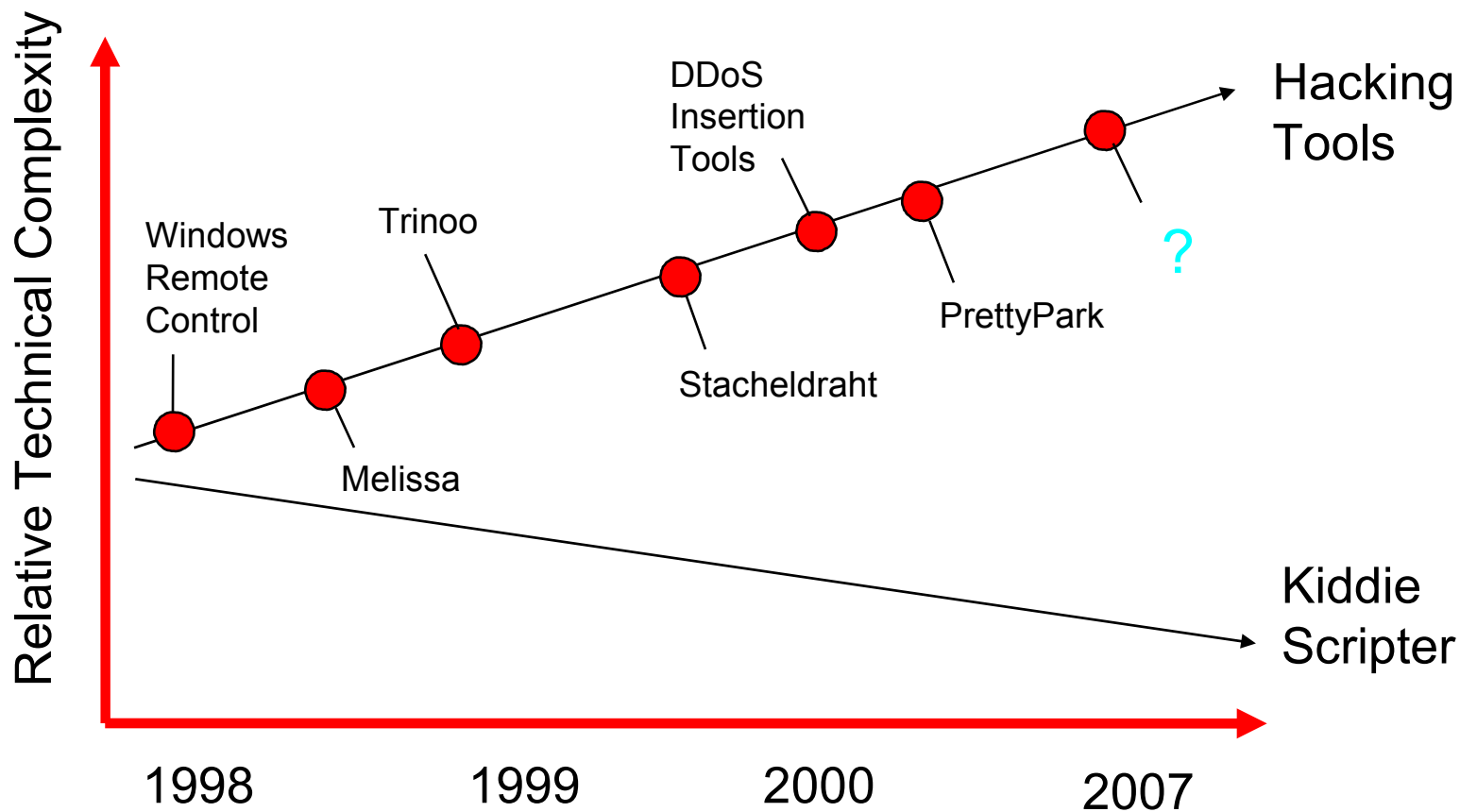
With 9.9 million victims last year alone, the FTC warned the thefts cost businesses \$48 billion and \$5 billion in out-of-pocket expenses to individuals in 2002.



Story Tools

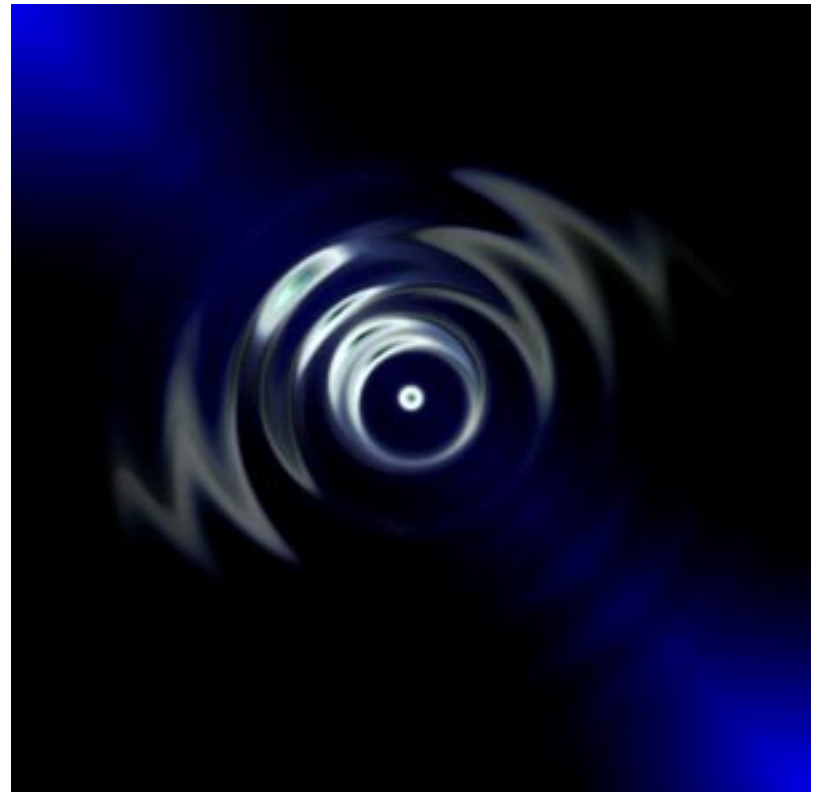
- [SAVE THIS](#)
- [E-MAIL THIS](#)
- [PRINT THIS](#)
- [MOST POPULAR](#)

Tren 20-Year Trend: Stronger Attack Tools



How Cyber Attacks have Evolved

1. Automation: increasing speed of attacks
2. Increasingly sophisticated attack tools
3. Faster discovery of vulnerabilities



Common Attacks

- ⊙ Backdoor
- ⊙ Bacteria
- ⊙ Buffer overflow/overrun
- ⊙ Compromised system utilities
- ⊙ E-mail forgery
- ⊙ E-mail relay
- ⊙ IP spoofing
- ⊙ Keystroke monitoring
- ⊙ Logic bomb
- ⊙ Mail bombing
- ⊙ Man in the middle
- ⊙ Masquerade
- ⊙ Network scanning
- ⊙ Packet sniffing
- ⊙ Password cracking
- ⊙ Ping flooding
- Replay attack
- Script kiddies
- Security audit tools
- Shell escapes
- Shoulder surfing
- Smurfing
- Social engineering
- SYN flooding
- Traffic analysis
- Trapdoor
- Trojan horse
- van Eck attack
- Virus
- War dialing
- Worm

Malware Increase 800%!!!



The amount of malware captured last year increased by 800 percent over 2006. The increase was substantial jump from 2006, when malware examples increased by 172 percent over 2005, according to Panda Security.

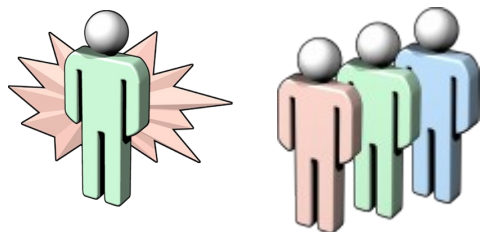
Researchers at the Madrid-based anti-virus vendor received an average of more than 3,000 strains of malware per day during 2007.

Ryan Sherstobitoff, chief corporate evangelist at Panda, told SCMagazine.com that 72 percent of networks tested by his company contained active threats and two percent were infected with malicious code.

Cybercriminals are attempting to flood network with more malware than the networks can handle, he said.

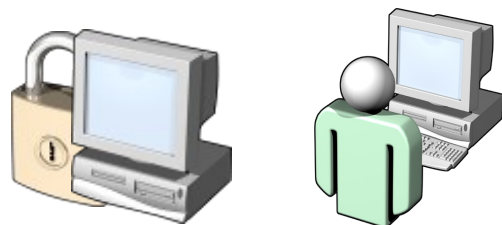
2009 increasing trends?

Challenges When Implementing Security



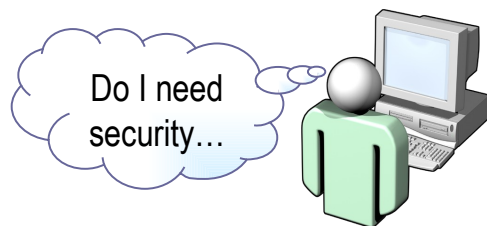
Attackers vs. Defenders

- Attacker needs to understand only one vulnerability
- Defender needs to secure all entry points
- Attackers have unlimited time
- Defender works with time and cost constraints



Security vs. Usability

- Secure systems are more difficult to use
- Complex and strong passwords are difficult to remember
- Users prefer simple passwords



- Developers and management think that security does not add any business value
- Addressing vulnerabilities just before a product is released is very expensive

Security As an Afterthought



Kesimpulan

Conclusion

- ① Security is a dynamic processes. NOT a DESTINATION but a JOURNEY.
- ① ICT Security keep changing from time to time..
...equip yourself.....then you'll be LESS worry....