Keamanan Jaringan

# 15. Gaining Access

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Anatomi Hacking

1.Footprinting

2.Scanning

3.Gaining Access/System Hacking

4.....

# Footprinting & Scanning

Informasi yang telah dikumpulkan sampai tahapan ini

- Alamat IP
- Sistem Operasi
- Hardware, Software
- Port dan service
- Username
- Alamat Email

# Gaining Access

System Hacking

Tujuan :

Mendapatkan akses ke komputer target

# System hacking – Teknik yg digunakan

- Cracking password
- Social Engineering
- Escalating priviledge
- Executing application
- Hiding files
- Covering track

Keamanan Jaringan

# 16. Password

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Password pada umumnya

- Mudah ditebak
- Jarang diganti
- Digunakan bersama untuk beberapa macam sistem
- Ditulis di tempat yang tidak aman

# Mencuri Password

1. Shoulder Surfing

# Menebak Password

Menebak password dari informasi yang diketahui tentang user

- Tanggal lahir
- Acara TV favorit
- Nomer telefon

# Social Engineering

- Penyerang mengaku sebagai teknisi perlu melakukan konfigurasi/update pada aplikasi yang digunakan di perusahaan tersebut.

- Karena harus melakukan update di jaringan, kemudian meminta user untuk memberitahu password yang digunakan untuk login di komputer

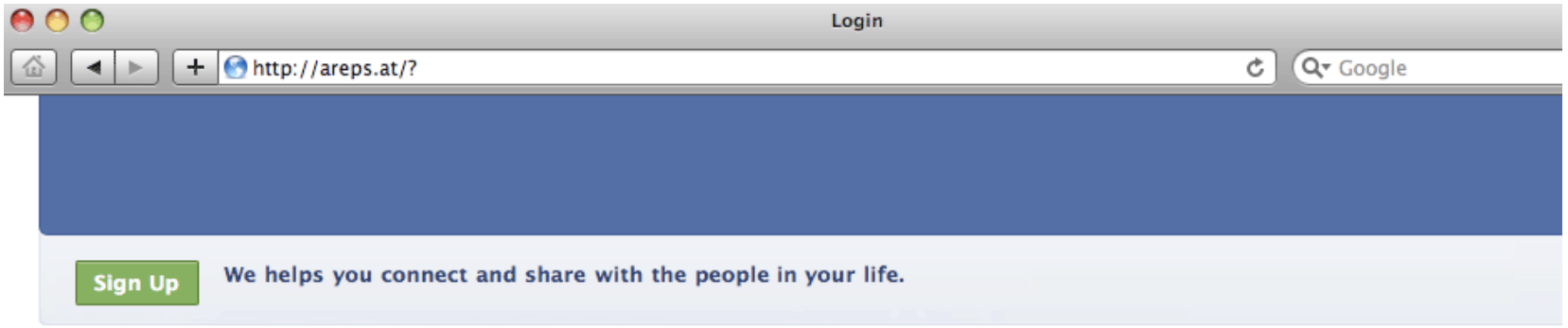
# Social Engineering + Keylogger

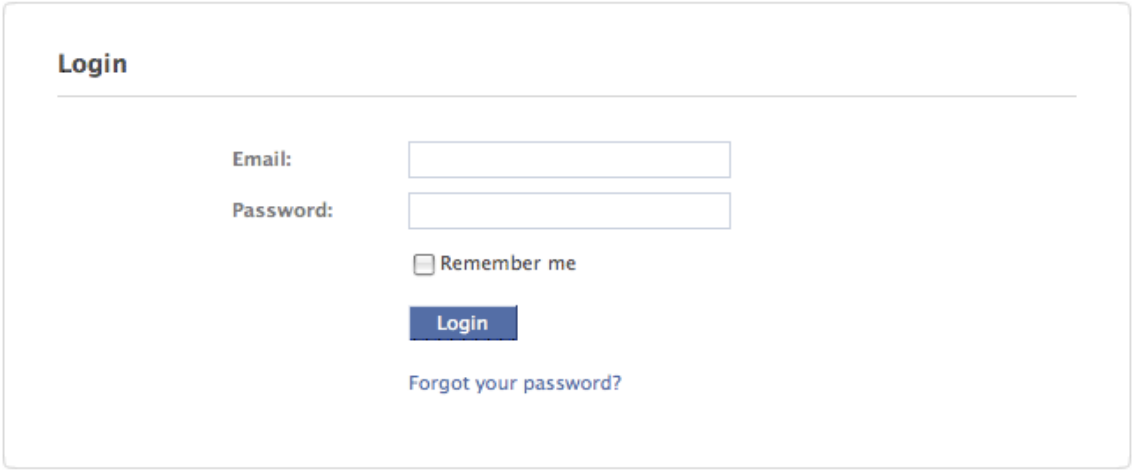
- Keylogger : aplikasi untuk mencatat aktifitas keyboard

- Eh nebeng ngeprint dong → pasang keylogger
- Kirim email, ini foto gw liburan → fotonya sudah ditempel keylogger

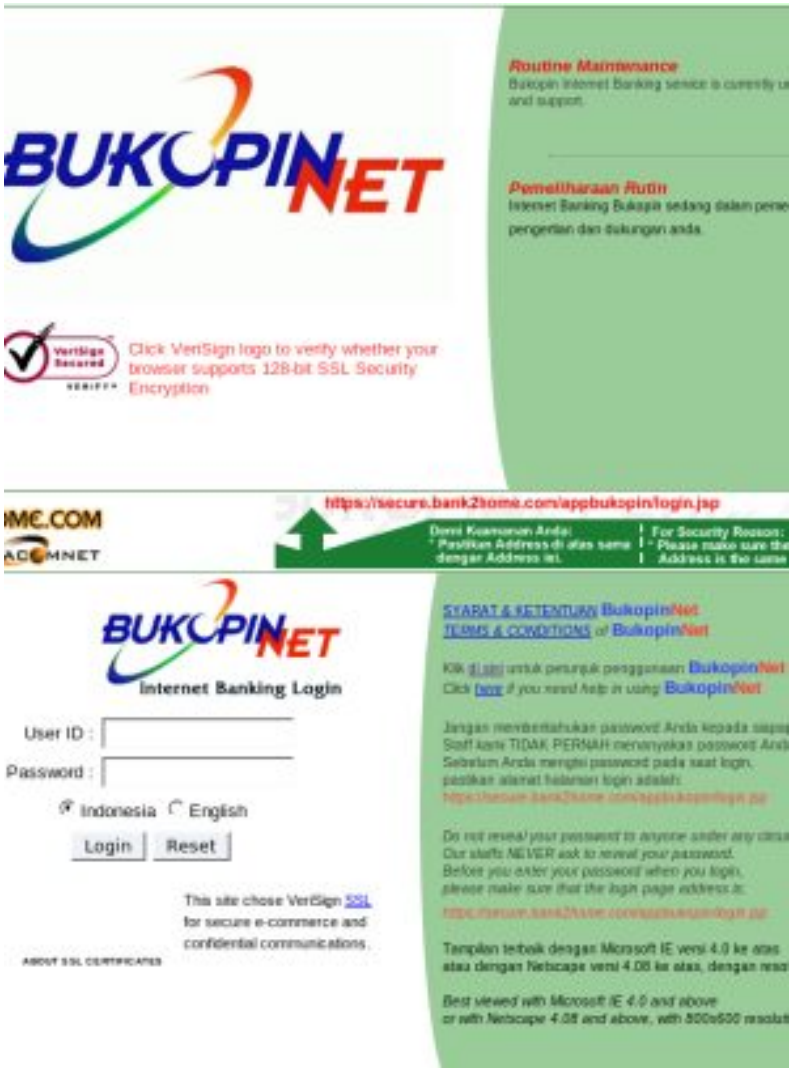
- Keylogger mencuri password

# Phishing


Login
http://areps.at/?
Google
Sign Up
We helps you connect and share with the people in your life.


Login
Email:
Password:
Remember me
Login
Forgot your password?

# Phishing


BUKOPINNET
Routine Maintenance
Pemeliharaan Rutin
Click VeriSign logo to verify whether your browser supports 128-bit SSL Security Encryption
https://secure.bank2home.com/appbukopin/login.jsp
BUKOPINNET
Internet Banking Login
User ID :
Password :
Indonesia
English
Login
Reset
This site chose VeriSign SSL for secure e-commerce and confidential communications.
SYARAT & KETENTUAN BukopinNet
TERMS & CONDITIONS of BukopinNet

Keamanan Jaringan

# 17. Cracking Password

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Cracking Password

- Dictionary Attack
- Brute-Force Attack

# Dictionary Attack

- *Dictionary Attack* dilakukan dengan cara membandingkan password dengan suatu *dictionary*
- *Dictionary = Kamus → wordlist*
- Daftar kata atau kemungkinan password
- Dijalankan menggunakan aplikasi password cracking

# Dictionary attack - 2

123456
Password
Qwerty
Abc123
123456789
111111
....
**Password list/ dictionary**

Login :
Password:

# Tools Password Cracking

- THC Hydra
- John the ripper
- Brutus
- Medusa
- Ophcrack
- Aircrack-ng

Keamanan Jaringan

# 18. Wordlist

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Wordlist

- =Dictionary
- =Bikin sendiri wordlist
- File text
- Isi dengan daftar kemungkinan password dari korban
- Informasi berasal dari proses footprinting

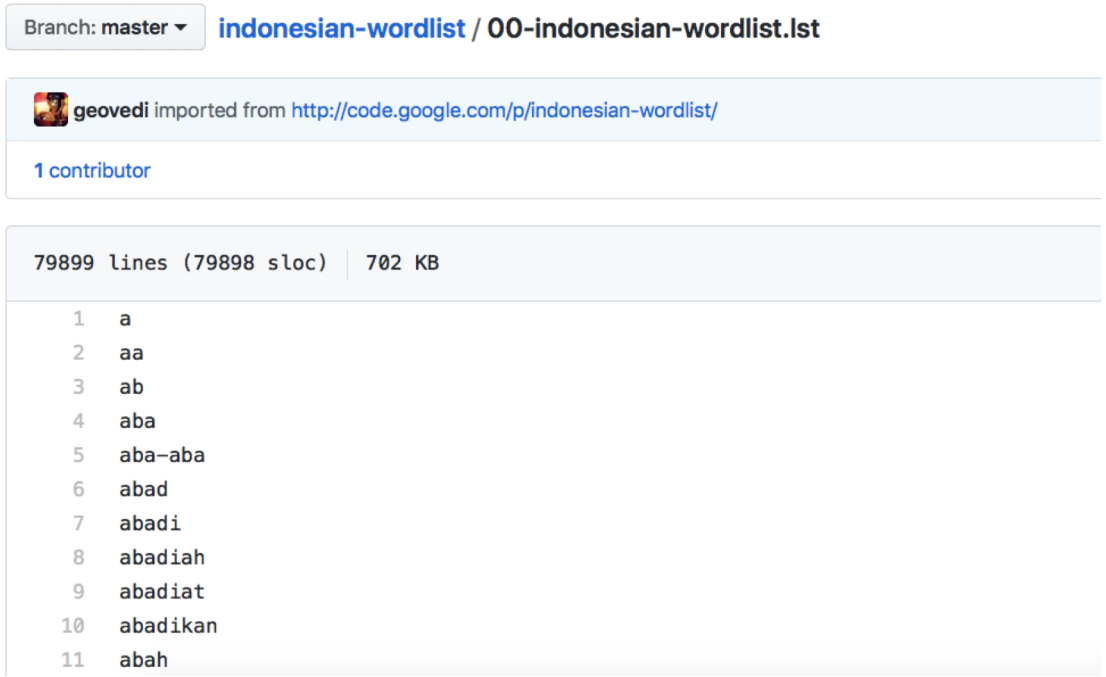
# Wordlist

- Googling: password wordlist
- https://github.com/danielmiessler/SecLists/tree/master/Passwords
- https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt

- Kali Linux default wordlist

# Wordlist - Indo

- https://github.com/geovedi/indonesian-wordlist



# Dictionary Attack

Kelemahan:

- Tergantung dari wordlist
- Semakin lengkap wordlist semakin baik
- Bahasa

Keamanan Jaringan

# 19. Brute Force

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Brute Force Attack

- *Brute Force Attack* dilakukan dengan cara mencoba semua kombinasi karakter yang mungkin
- Misal untuk 3 karakter

aaa
aab
aac
aad
.....
ZZZ

Login :
Password:

# Tools Password Cracking

- THC Hydra
- John the ripper
- Brutus
- Medusa
- Ophcrack
- Aircrack-ng

# Port Target

- SSH
- Telnet
- FTP
- VNC
- Remote Desktop

# Estimasi waktu yang dibutuhkan

- abcdefg - 7 karakter - 0,29 detik
- abcdefgh - 8 karakter - 5 jam
- abcdefghi - 9 karakter - 5 hari
- abcdefghij - 10 karakter - 4 bulan
- abcdefghijk - 11 karakter - 10 tahun

Keamanan Jaringan

# 20. Teknik Cracking Lainnya

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Teknik Cracking Password Lainnya

Hash Cracking

- Password disimpan dalam bentuk Hash
- Hash : teknik kriptografi
  - MD5, SHA1, SHA 256 dll
- Penyerang mencari file hash password
- Mencari database password hash – rainbow table
- Tools: Winrtgen

# Sniffing

- Menangkap password di trafik jaringan
- Penyadapan
- Tools: Cain & Abel
- Pertemuan berikutnya

# Default Password

- Perangkat jaringan dikonfigurasi dengan default password
- Diset dari Pabriknya
- Harusnya diganti

- Tools:
- Cirt.net

# Teknik Lainnya

- Man-in-the-middle attack
  - SSL Strip, Burp Suite, BEEF (Browser Exploitation Tools)
- Hash Injection
  - Masuk dulu ke sistem
  - Mencuri Hash Password;
- Session Hijacking
  - Cookies pada jaringan
- USB Drive → Passview

Keamanan Jaringan

# 21. Keamanan Password

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

# Cracking Password

- Dictionary attack
- Brute-Force Attack
- Teknik Lainnya

- Ternyata ada banyak sekali cari untuk meretas password
- Bagaimana untuk mengamankan password?

# Tips Password

Hindari menggunakan password yang lemah

- 123456
- Password
- Qwerty
- Abc123

- Worst Password List

# Tips

- Makin Panjang makin bagus: minimum 12 karakter
- Kombinasi Karakter:
  - huruf kecil, huruf besar, angka, simbol
- Kombinasi beberapa kata atau kalimat
- Tools random password generator

# Tips Password

- Ganti Password anda secara rutin
- Jangan gunakan password yang sama pada setiap layanan yang berbeda
- Jangan simpan password di browser / aplikasi

# Referensi


Buku Bacaan Wajib (BW)

Engebretson, P. (2011). *The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress.

Stallings, W. (2010). *Network Security Essentials:Applications and Standards 4th Edition.* Prentice Hall.

Buku Bacaan Anjuran (BA)

Harris, S. (2010). *CISSP All in One Exam Guide, 5th Edition.* McGraw Hill.

Walker, M. (2010). *CEH Certified Ethical Hacker All-in-One.* McGraw Hill.