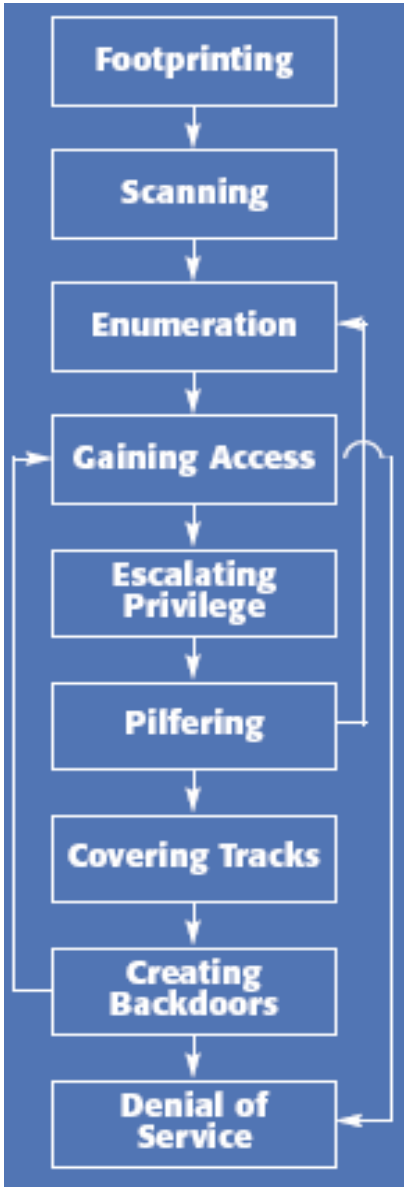
Eksploitasi Keamanan

Eksploitasi Keamanan

- Anatomi suatu serangan hacking
- 1. Footprinting
- Mencari rincian informasi terhadap sistemsistem
- untuk dijadikan sasaran, mencakup
- pencarian informasi dengan *search engine,*
- whois, dan DNS zone transfer.
- **Hacking Tools**
- **• whois, host, nslookup, dig (tools di sistem**
- UNIX)
- **• Sam Spade (tools di sistem Windows)**
- http://www.samspade.org.
- **• ARIN, Traceroute, NeoTrace, VisualRoute**
- Trace, SmartWhois, Visual Lookout,
- VisualRoute Mail Tracker,
- eMailTrackerPro



Eksploitasi Keamanan

- 2. Scanning
- • Terhadap sasaran tertentu dicari pintu masuk
- yang paling mungkin. Digunakan *ping sweep dan port scan.*
- • Mencari informasi mengenai suatu alamat IP dapat
- menggunakan beberapa software seperti
- 1. WinSuperKit - http://www.mjksoft.com
- 2. Ping Plotter - www.pingplotter.com
- 3. SuperScan
- 4. UltraScan
- 5. Lain-lain

Eksploitasi Keamanan

- 3. Enumeration.
- Telaah intensif terhadap sasaran, yang mencari *user*
- *account absah, network resource and share, dan aplikasi*
- untuk mendapatkan mana yang proteksinya lemah.
- 4. Gaining Access.
- Mendapatkan data lebih banyak lagi untuk mulai mencoba
- mengakses sasaran. Meliputi mengintip dan merampas
- password, menebak password, serta melakukan *buffer*
- *overflow.*

Eksploitasi Keamanan

- 5. Escalating Privilege.
- Bila baru mendapatkan *user password di tahap*
- sebelumnya, di tahap ini diusahakan mendapat privilese
- admin jaringan dengan *password cracking atau exploit*
- sejenis getadmin, sechole, atau lc_messages.
- 6. Pilfering
- Proses pengumpulan informasi dimulai lagi untuk
- mengidentifikasi mekanisme untuk mendapatkan akses ke
- *trusted system. Mencakup evaluasi trust dan pencarian*
- *cleartext password di registry, config file, dan user data.*

Eksploitasi Keamanan

- 7. Covering Tracks
- • Begitu kontrol penuh terhadap sistem diperoleh,
- maka menutup jejak menjadi prioritas.Meliputi
- membersihkan *network log dan penggunaan hide tool*
- seperti macam-macam *rootkit dan file streaming.*
- • Hacking Tool
- Dump Event Log, elsave.exe, WinZapper, Evidence
- Eliminator

Eksploitasi Keamanan

- 8. Creating Backdoors.
- Pintu belakang diciptakan pada berbagai bagian dari
- sistem untuk memudahkan masuk kembali ke sistem ini
- dengan cara membentuk *user account palsu,*
- menjadwalkan *batch job, mengubah startup file,*
- menanamkan servis pengendali jarak jauh serta
- *monitoring tool, dan menggantikan aplikasi dengan trojan.*

Eksploitasi Keamanan

- **9. Denial of Service.**
- Bila semua usaha di atas gagal, penyerang
- dapat melumpuhkan sasaran sebagai usaha terakhir.
- Meliputi SYN flood, teknik-teknik ICMP, Supernuke,
- land/latierra, teardrop, bonk, newtear, trincoo, smurf, dan
- lain-lain.
- Hacking Tools
- Jolt2, Bubonic.c, Land and LaTierra, Targa

Eksploitasi Keamanan

- Klasifikasi DoS Attack
- • Smurf, Buffer Overflow Attacks
- • Ping Of death
- • Teardrop
- • SYN
- • Tribal Flow Attack

TERIMA KASIH

1. Mencari informasi dengan *search engine, whois, dan DNS* zone transfer merupakan aktifitas ...
   a. Footprinting c. Pilfering
   b. Enumeration d. Gaining Access

2. Mengintip, merampas dan menebak password, serta melakukan *buffer overflow, merupakan aktifitas …*
   a. Footprinting c. Pilfering
   b. Enumeration d. Gaining Access

3. Pencarian *cleartext password di registry, config file, dan user data merupakan aktifitas …*
   a. Footprinting c. Pilfering
   b. Enumeration d. Gaining Access

SOAL-SOAL LATIHAN

4. Berikut ini adalah software yang digunakan untuk dapat melumpuhkan sasaran sebagai usaha terakhir, kecuali ...
   a. Supernuke
   b. Superscan
   c. teardrop
   d. newtear

5. Mencari informasi mengenai suatu alamat IP dapat meng gunakan beberapa software seperti berikut, kecuali....
   a. WinSuperKit
   b. SuperScan
   c. Ping Plotter
   d. Teardrop