MENYERANG DAN BERTAHAN

Mengetahui Bagaimana Hackers Beraksi dan Membangun Pertahanan yang Kuat Pada Sistim dan Jaringan Komputer

n e g a t i v e

information security engineer

negative@magnesium.net

12/07/2003

whoami

- 4 c0mpv73r 633k ;-)
- Information Security Engineer
- Security Evangelist
- FreeBSD & OpenBSD Developer
- Natural Born Junker
- a monkey
- ... you name it

Fokus Presentasi

- mengenal hackers, crackers, blackhat, whitehat
- ethical hacking
- network mapping, scanning, fingerprinting
- vulnerability assessment
- eksploitasi sistim target (remote & local)
- backdoors, trojan horses, rootkits
- membangun sistim pertahanan yang baik

Hackers, Crackers, Blackhat, Whitehat

- hackers:
  - tukang ngoprek yang selalu penasaran
- crackers:
  - pembobol sistim / aplikasi
- blackhat:
  - hacker yang jahat
- whitehat:
  - hacker yang baik

Hacking (pro dan kontra)

- etika hacking
  - pro: semua informasi adalah free
  - kontra: jika semua informasi adalah free, tidak ada lagi privacy
- aspek security
  - pro: intrusion adalah ilustrasi kelemahan sistim
  - kontra: tidak perlu jadi pencuri untuk menunjukkan pintu yang tidak terkunci
- idle machines
  - pro: hacking hanya pada idle machines
  - kontra: idle machines milik siapa?
- science education
  - pro: hanya membobol tapi tidak merusak
  - kontra: newbie tidak pernah tau apa yang dapat mereka lakukan

Mengapa Perlu Tahu Teknik Hacking?

- mengetahui sudut pandang hackers terhadap security
  - know your enemies
- meningkatkan kewaspadaan staff IT
  - kita tidak pernah tahu kapan hackers akan menyerang
- meningkatkan respon terhadap insiden
  - bagaimana melakukan respon yang baik

Kelemahan Protokol TCP/IP

- target spoofing
  - X adalah kekasih Y, dan Z berpura-pura menjadi X
- session hijacking
  - X menelpon Y, dan Z mengambil-alih percakapan
- dapat dimanipulasi
  - Y kirim parsel ke X, dan Z mengganti isi parsel dengan bom
- Denial of Service (DoS)
  - Jalan ke rumah Y hanya muat 1 mobil, Z memarkirkan 4 mobil memenuhi jalan agar X tidak dapat berkunjung ke rumah Y

Metodologi Hacking (1/4)

- Buffer Overflow Attacks
  - Victim adalah aplikasi yang ditulis dengan tidak baik
  - Memanfaatkan kesalahan programming untuk mengeksekusi sisipan code
  - Dapat dieksploitasi secara remote atau local, tergantung aplikasi
  - Spesifik pada Processor & Operating System tertentu
- Denial of Service
  - Menjadikan service tidak dapat dipergunakan
  - Target DoS:
    - koneksi jaringan penghubung antar service dan user
    - sistim operasi yang digunakan
    - aplikasi yang menyediakan service

Metodologi Hacking (2/4)

- Distributed Denial of Service (DDos) Attacks
  - Sama seperti DoS, namun menggunakan banyak hosts untuk menyerang satu target
  - Hosts yang digunakan untuk menyerang biasanya hosts yang telah berhasil dikuasai
  - Eksekusi DDoS dilakukan secara bersama-sama (menggunakan master hosts)
  - Efek yang ditimbulkan lebih berbahaya

Metodologi Hacking (3/4)

- Penyalahgunaan Trust
  - Hanya berlaku pada jaringan berskala kecil dan menggunakan tipikal arsitektur jaringan yang lama
  - Memanfaatkan trust antar hosts / systems
  - Sulit dibedakan antara intruder dan user biasa
- Brute Force Attacks
  - Secara berulang melakukan percobaan otentifikasi
  - Menebak username dan password
  - Mengcrack shadow password file

Metodologi Hacking (4/4)

- CGI / WWW Attacks
  - Terbagi dalam 3 (tiga) kategori:
    - buffer overflow: tidak melakukan validasi pada user input
    - command execution: dapat mengeksekusi perintah tambahan
    - subverting client-side scripting: dapat dimanfaatkan untuk mengeksekusi buffer overflow dan command execution disisi client
- Backdoors & Trojans
  - Memperdayai user atau sysadmin untuk memberikan password mereka tanpa diketahui
  - Dapat berupa program yang umum dikenal dan sering digunakan sehingga tidak menimbulkan kecurigaan

Hacking Tools

- Scanners
  - mengidentifikasi sistim target
  - mencari vulnerability holes
- Exploits
  - memanfaatkan vulnerability holes
  - mendapatkan akses penuh (UNIX: root)
- Backdoors, Trojan Horses, dan Rootkits
  - membuat jalan masuk tersembunyi
  - menghapus jejak
  - mengelabui sistim administrator
- Password Crackers
  - mengcrack shadow password

Mencari & Mengumpulkan Informasi

- Secara aktif
  - portscanning
  - network mapping
  - OS detection
  - applications fingerprinting
- Secara pasif
  - via Internet Registry (domain, IP Address)
  - website target
  - mailing-list

Network Scanning

- Menginterpretasikan informasi yang sudah didapat mengenai sistim dan jaringan target
  - membandingkan informasi yang sudah didapat (domain/hostname) dengan kenyataan
- Mengidentifikasi hosts yang aktif
  - dapat menjadi target attack
- Memetakan struktur jaringan target
  - membuat struktur jaringan target
  - dapat mencari tahu hosts yang tidak dilindungi dengan baik
- Mencari hosts yang vulnerable
  - mengidentifikasi service, dan membandingkannya dengan database exploit yang dimiliki

Vulnerability Assessment

- Mencari informasi vulnerability holes dan exploits
  - Website: PacketStormSecurity (packetstormsecurity.com)
  - IRC: trading 0-day? (#darknet/efnet)
  - Mailing-list: BUGTRAQ, Full-Disclosure
- Exploit testing
  - di mesin sendiri
  - di mesin orang lain yang telah dikuasai terlebih dahulu

Mendapatkan Akses

- Mengeksploitasi vulnerability holes
  - remote host

```
$ gcc -o exploit exploit.c; ./exploit -t www.xyz.co.id
# hostname; id
webserver.xyz.co.id
uid=0(root) gid=0(wheel) groups=0(wheel), 1(daemon), 2(kmem), 3(sys)
```

  - local host

```
$ gcc -o exploit exploit.c; ./exploit
# hostname; id
localhost.localdomain
uid=0(root) gid=0(wheel) groups=0(wheel), 1(daemon), 2(kmem), 3(sys)
```

- Social Engineering
  - memperdayai user untuk memberitahukan username dan password (kasus Kevin Mitnick)
  - mengamati seseorang memasukkan username dan password

```
******** -> abicakep
```

- Bruteforcing Username & Password

Mengelabui Firewall dan IDS

- Menggunakan protokol firewall-friendly
  - semua hosts umumnya mengijinkan port 80 (www), intruder menggunakan port tersebut untuk mengirimkan shellcodes
  - connect-back shellcode
    - firewall memblokir semua koneksi yang masuk, intruder menggunakan connect-back shellcode untuk mengaktifkan koneksi pasif

      `X -/-> Y; X <-- Y`
- IDS evasions
  - polymorphic shellcode

Apa yang Dilakukan Hackers Selanjutnya?

- Menginstall Backdoors, Trojan Horses, dan Rootkits
  - memudahkan akses masuk kembali
  - memperdayai sysadmin untuk mendapatkan akses penuh (root)
  - menginstal sekumpulan tools untuk menjadi invisible ketika login
- Menghapus Jejak
  - memodifikasi logfiles sehingga tidak menimbulkan kecurigaan sysadmin
- Menyalin `/etc/passwd` & `/etc/shadow` atau `/etc/master.passwd`
  - diperlukan sewaktu-waktu jika semua backdoor terhapus

Membangun Pertahanan (1/4)

- Secure Network Design
  - penggunaan switch untuk menghindari network sniffing
  - membagi jaringan berdasarkan klasifikasi penggunaan
    - bedakan antara kelas server dengan kelas workstation
    - menempatkan firewall, IDS pada posisi yang tepat
- Implementasi Security Policy
  - berhubungan dengan user
  - berkaitan pada penggunaan sistim dan jaringan
  - harus diawasi dengan benar

Membangun Pertahanan (2/4)

- Firewall
  - commercial vs opensource
  - konfigurasi firewall
    - block all vs permit all
- Intrusion Detection System (IDS)
  - commercial vs opensource
  - Network Intrusion Detection System (NIDS)
  - Host-based Intrusion Detection System (HIDS)

Membangun Pertahanan (3/4)

- Security Monitoring
  - berkaitan dengan policy
  - mengamati anomali event
- Secure Logging
  - logging itu perlu
  - mengamankan log dari manipulasi
- System Hardening
  - menggunakan kernel security patch
  - menonaktifkan service yang tidak perlu
  - melokalisasi vulnerable program dengan chroot atau jail

Membangun Pertahanan (4/4)

- Security Audit
  - memeriksa status service dan sistim secara berkala
  - membandingkan versi aplikasi dengan versi terbaru
- Penetration Testing
  - ethical hacking?
  - menyewa hacker (atau ex-hacker)?
  - melakukan test pembobolan dan eksploitasi service
  - memberikan advisori terhadap setiap titik rawan

TANYA - JAWAB

Format presentasi yang dapat diprint tersedia di:
`http://www.magnesium.net/~negative/talks/hacking-and-defense.pdf`

Materi disusun oleh: negative, sakitjiwa. Dipresentasikan oleh: negative