Keamanan Jaringan

29. Keamanan Wireless

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Wireless

- Wireless vs Wired Popular
- Wireless semakin Popular
- Kemudahan akses
- Instalasi Mudah, murah
- Wifi
- Keamanan ?

Wifi

- Akses Poin (AP) : perangkat jaringan
- SSID : Nama Akses Poin
- BSSID : alamat MAC Akses Poin

Standar WLAN

- 802.11
- PC, Game konsol, smartphone, tablet, printer,
- 802.11 a/b/g/n

Standard	Frequency	Modulation	Speed
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	DSSs	11 Mbps
802.11g	2.4 GHz	OFDM , DSSS	54 Mbps
802.11n	2.4 , 5 GHz	OFDM	54 Mbps

Enkripsi Wireless

- WEP
- WPA
- WPA2
- WPA3 ?

Encryption	Encryption Algorithm	IV Size	Encryption Key	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-Bits	CRC-32
WPA	RC4 , TKIP	48-bits	128-Bits	Michael Algorithm and CRC-32
WPA2	AES , CCMP	48-bits	128-Bits	CBC-MAC

Wifi Hacking

- Mencari Wifi
  - Airwaves, Netsurveyor, inSSIDer, Vistumbler, Netstumbler
- Analisa Trafik
  - Nama SSID, Metoda Autentikasi, Teknik Enkripsi
  - Wireshark/Pilot Tool, Omni Peek, Commview, dll
- Serangan
  - Aircrack-ng

Keamanan Jaringan

30. Wireless Cracking

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Aircrack-ng

- Windows, Linux
- Deteksi AP, sniffer, WPA cracker
- Airmon-ng
- Airodump-ng
- Aireplay-ng
- Airdrop-ng

Crack WPA

1. Monitor trafik wireless
   - airmon-ng start eth1 (perangkat jaringan kita)
2. Mengumpulkan data
   - Airodump-ng –write capture eth1

```
C:\>airmon-ng start eth1
C:\>airodump-ng –write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3      0    1   54e OPN                   IAMROGER
02:24:2B:CD:68:EE  99   9    75       2      0    5   54e WPA  TKIP    PSK   COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0      0    9   54e WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1      0    11  54e WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1 - 0  0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

Crack WPA

3. Deauthenticate client
   - Aireplay-ng deauth 11 –a Mac address

4. Cracking password
   - Aircrack-ng.exe –a 2 –w capture.cap (nama file)

Jenis Serangan Wireless

- Spoofing Mac Address
- Rogue Access Point (RAP)
- Session Hijacking
- Man-In-the-midle Attack
- Dos Attack
- Jamming

Defend Wireless

- WIPS – Wireless Intrusion Prevention System
- WiFi Audit
  - Airmagnet Wifi Analyzer, Motorola AirDefense Service Platform (ADSP) ,Cisco Adaptive Wireless IPS, Aruba RF Project
- Enkripsi → WPA2
- Kompleksitas Password
- MAC Filtering
- RF Scanning

Keamanan Jaringan

31. Keamanan Web

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Web Server

- Apache : 57,9%
- Nginx : 23,7%
- IIS : 13,2%
- LiteSpeed : 2,2%
- Google Server : 1,3%
- dll

Serangan Web Server

- DoS/DDoS
- DNS Hijack
- DNS Amplification
- Directory Traversal
- Sniffing
- Deface
- Http response splitting attacng
- Web cache poisoning attackg
- SSH Brute Force
- Phishing

Tahap serangan

- Information Gathering
  - Social engineering, robots.txt
- Footprinting
  - Netcraft, Maltego, httprecon, ID Serve
- Mirroring website
  - Httrack, blackwidow, webcopier
- Vulnerability scanning
- Password Cracking
- Session Hijacking
- Tools: Metasploit, Wfetch, Hydra, Brutus

Defense

- DMZ
- Firewall
- IDS, IPS
- Pembatasan Port
- Port 443 HTTPS
- Enkripsi Trafik
- Certificate server

- Secure Coding
- Disable tracing
- Disable debug compile
- Kebijakan Password
- Patch Management
- Update
- Account Management

Tools

- MBSA (Microsoft Baseline Security Analyzer)
- Syhunt Hybrid
- WebsiteCDS
- UrlScan
- N-Stalker WebApp Scanner
- Wikto
- Acunetix
- HackAlert
- QualsysGuard

Keamanan Jaringan

32. Keamanan Aplikasi Web

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Statistik serangan Website

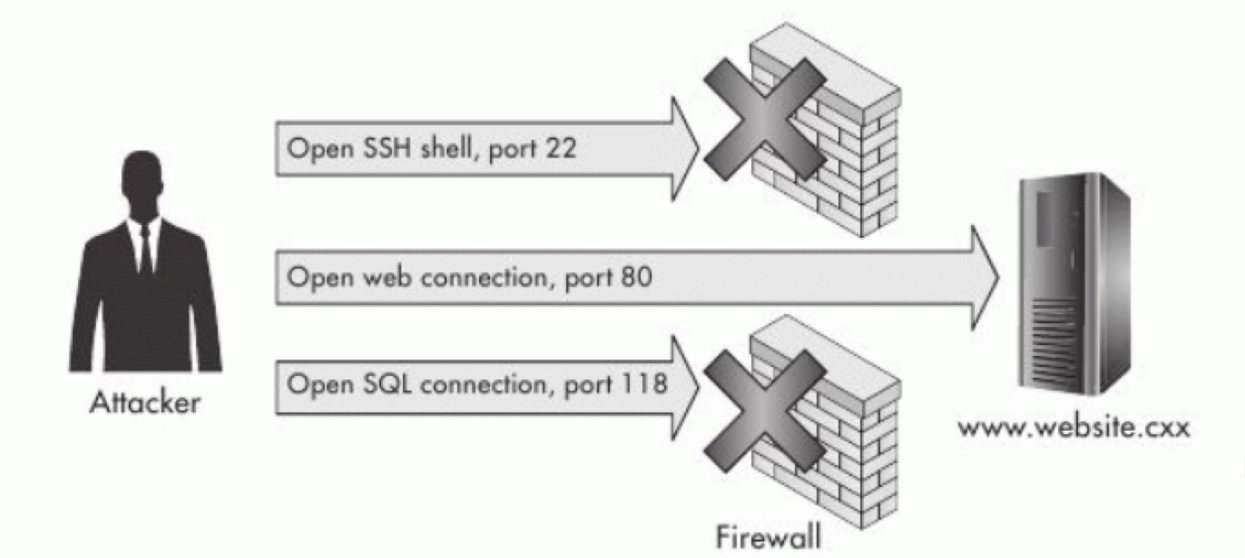
- 30 ribu web diretas setiap harinya
- Ribuan tools hacking web tersedia di internet secara free
- 70% serangan di internet dari aplikasi web

Kasus Peretasan Web Sony

- Serangan SQL Injection web Sony oleh LulzSec
- 2011
- 77 juta data user bocor
- 1 bulan dinon aktifkan
- Kerugian $171 Juta

Mitos tentang Firewall

- Kami aman karena punya Firewall
- Tutup port
- Penyerang bisa menggunakan Aplikasi Web untuk memulai serangan



Aplikasi Web

- Aplikasi yang menyediakan interface antara pengguna dan web server
- Memudahkan pengguna mengakses data di server
- Memiliki berbagai celah keamanan
- Bisa dimanipulasi oleh penyerang untuk meretas sistem

Resiko Aplikasi Web

- Deface: Mengganti tampilan web
- Install malware, botnet
- Mengambil alih Sistem

Keamanan Jaringan

33 Serangan Web

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

OWASP TOP 10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Component with known Vulnerability
10. Insufficient Logging & Monitoring

OWASP

- Open Web Application Security Project
- Proyek Open source → Meningkatkan keamanan aplikasi web
- Kontributor Individu, Perusahaan, Relawan
- Secure Coding, library
- Tools, scanner, lab vulnerable
- Daftar Top Ten

Injection

Jenis-Jenis Injection

- SQL Injection
- Command Injection
- LDAP Injection

Dampak serangan

- Bypass Login
- Menampilkan Data Rahasia
- Merubah Data
- Menghapus Database
- Menjalankan Perintah secara remote

SQL Injection

- Bypass Login
- Manipulasi Query
- "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";
- Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" + request.getParameter("id") + "'");
- http://example.com/app/accountView?id=' or '1'='1

SQL Injection Tools

- BSQL Hacker
- Marathon Tool
- SQL Power Injector
- Havij
- Sqlmap
- Sql brute

Keamanan Jaringan

34. XSS Attack

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Cross-Site Scripting (XSS)

- Penyerang memasukan Script Jahat ke halaman Web Target

Contohnya pada:

- bagian komentar pada blog,
- Memodifikasi link URL, meminta korban membuka link tersebut

Penyebab

- Tidak dilakukan validasi Input

Script XSS

- Javascript
- VBScript
- ActiveX
- HTML
- Flash

Dampak Serangan XSS

- Redirect korban ke halaman tertentu
- Mencuri data
- Merubah data di server
- Meretas Password
- Menjalankan skript jahat
- Menampilkan pop up tertentu
- Penyadapan data korban

Tools Pengujian

- Burp Suite
- Cookie Digger
- WebScarab
- PowerSploit
- BeEF

Keamanan Jaringan

35. Pencegahan Serangan Web

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Pencegahan

1. Validasi Input
2. Filter Paket dengan WAF, IDS
3. Drop ICMP
4. Matikan service & port tidak perlu
5. Patch Sistem
6. Sanitasi Input
7. Uji SQL Injection
8. Minimisasi aplikasi pihak ketiga

Pencegahan (2)

9. Akses ke Database menggunakan akun non-privileged
10. Gunakan prosedur store & query parameter
11. Batasi akses ke database, tabel dan kolom
12. Batasi pesan error yang ditampilkan
13. Lakukan pengujian sistem
14. Analisa Source code
15. Matikan perintah shell

Security Tool

- Acunetix
- Watcher Web
- Netsparker
- N-Stalker Scanner
- VampireScan
- OWASP ZAP

Web Application Firewall

- dotDefender
- *Serverdefender VP*
- *Modsecurity*
- *ThreatSentry*
- *Radware*
- *QualsysGuard WAF*

Langkah Pengujian

- Information Gathering
- Pengujian konfigurasi
- Pengujian Autentikasi
- Pengujian Session
- Pengujian Autorisasi
- Validasi Data
- Pengujian DoS
- Web Service
- Ajax

Tools Pengujian

- Metasploit
- Browser Exploitation Framework (BeEF)
- PowerSploit

Terima Kasih

Materi Berikutnya:

Kajian 2
Teknik Pertahanan
Kriptografi

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.