Keamanan Jaringan

08. Teknik Penyerangan

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Motif Penyerangan

- Mencuri Data
- Mengubah Data
- Merusak
- Motif Politik atau ideologi
- Balas Dendam
- Bisnis

Tren Ancaman Serangan

- Cloud Computing
- APT (Advance Persistent Threat)
- Malware
- Perangkat Mobile
- Insider Attack
- Botnet

Masih ingat?

1. Computer Security
2. Application Security
3. Network Security

Masing-masing mempunyai tipe serangan dan cara pengamanan yang berbeda

Contoh Serangan pada Jaringan (Network)

1. Information Gathering
2. Sniffing & Eavesdropping
3. Spoofing
4. Session Hijacking
5. Man-In-the-Middle Attack
6. DNS & ARP Poisoning
7. Password-Cracking
8. Denial of Service
9. Compromised Key Attack
10. Serangan pada Firewall & IDS

Terima Kasih

Materi Berikutnya:

Anatomi Hacking

Keamanan Jaringan

09. Anatomi Hacking

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Hacker?

- Black Hat
- White Hat
- Grey Hat
- Suicide Hacker

- Cyber Terrorist
- State-Sponsored Hacker
- Script Kiddies
- Hacktivist

Tahapan Hacking / Anatomi Hacking

- Reconnaisance / Footprinting
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Track

Reconnaissance

- Tahap Persiapan
- Mengumpulkan Informasi sebanyak mungkin tentang target
  - Konfigurasi jaringan
  - Sistem yang digunakan
  - Jumlah user
- Teknik reconnaissance (berdasarkan interaksi dengan target)
  - Passive Reconnaissance
  - Active Reconnaissance

Scanning

- Scanning : pengujian (probe) atas suatu host memakai tools secara otomatis dengan tujuan mendeteksi kelemahan pada host tujuan
- Mengumpulkan Informasi tentang target
  - Komputer yang aktif
  - Port yang terbuka
  - Sistem Operasi
  - Perangkat jaringan
- Informasi akan berguna untuk menentukan Teknik penyerangan
- Tools :Port scanner, vulnerability scanner, dll

Gaining Access

- Mencari cara untuk mendapatkan akses ke sistem target
- Teknik yang digunakan:
  - escalating privilege
  - Password cracking
  - Buffer overflow
  - Session Hijacking
  - Denial of service
  - dll

Maintaining Access

- Mencuri Informasi
- Mengirimkan data-data korban ke penyerang
- Merubah data
- Merubah konfigurasi sistem
- Memasang backdoor, rootkit, Trojan

Clearing Track - Menghapus Jejak

- Menyembunyikan identitas penyerang
- Menghapus jejak
- Mencegah deteksi sistem pertahanan
- Merubah log:
  - sistem,
  - Server
  - Aplikasi

Terima Kasih

Materi Berikutnya:

Footprinting & Reconnaisance

Keamanan Jaringan

10. Footprinting & Reconnaissance

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Skill dasar yang diperlukan

- Sistem Operasi (Windows, Linux, Unix, Mac)
- Jaringan
- Hardware
- Software
- Programming
- Pengetahuan tentang berbagai macam serangan

Footprinting

- Mengumpulkan informasi tentang sistem komputer target
- Arsitektur sistem

Teknik Footprinting

- Search Engine
- Advance Google Hacking
- Social Media
- Website
- Email
- Intelligence
- Whois
- DNS
- Network footprinting
- Social Engineering

Tools Footprinting

- Google
- Bing
- Netcraft.com
- Shodan.io
- Google Maps
- Privateeye.com
- beenverified.com
- Linkedin.com
- Google.com/finance
- Groups, Forum, Community

Advance Google Hacking Technique

- Site:
- Cache:
- Link:
- Allintext:
- Intext:
- Allintitle:
- Intitle:
- Allinurl:

- www.google.com/advanced_search
- https://www.exploit-db.com/google-hacking-database

Terima Kasih

Materi Berikutnya:

Footprinting Lanjutan

Keamanan Jaringan

11. Footprinting Lanjutan

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Footprinting Website

Untuk Mengetahui:

- Software yang digunakan
- Sistem operasi
- Database
- Subdirektori

Tools: Burp Suite, Zaproxy, Website Informer, Netcraft, Shodan, Web Data Extractor, WinHTTrack, Wayback Machine, dll

Email Footprinting

- Melacak alamat tujuan, IP pengirim, Server pengirim, Waktu pengiriman, sistem autentikasi email pengirim
- Tools :
  - PoliteMail
  - Email Tracker
  - Email Lookup

Whois

Nama Domain, Nama Pemilik, Alamat IP, DNS dll

- Whois.com
- Whois.domaintools.com
- Smartwhois
- Dnssniffers.com

Network Footprinting

Untuk mengetahui:

- Range Alamat Jaringan komputer target
- Hostname
- Sistem Operasi

Tools

- Traceroute
- Maltego
- Recon-ng

Terima Kasih

Materi Berikutnya:

Scanning

Keamanan Jaringan

12. Scanning

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Tujuan Scanning

Untuk mengetahui :

1. Komputer yang hidup pada suatu jaringan
2. Port yang terbuka
3. Sistem operasi komputer target
4. Service apa yang berjalan pada komputer target
5. Ada Firewall?
6. Celah keamanan target

NMAP

Tools untuk melakukan scanning

1. Untuk mengetahui apakah komputer target hidup? nmap –sP –v (IP target/range IP)
2. Untuk scan port tertentu! Nmap –sP –PE –PA (nomor port) (alamat IP)
3. Scan Sistem operasi: nmap –O (alamat IP)

tools lain: Zenmap, hping3, NetScan Tools Pro, Network Scanner, Fing, Network Discovery, Port Droid

Teknik Scanning

- TCP Connect: nmap –sT (alamat IP)
- Stealth scan: nmap –sS (alamat IP)
- Xmas scan : nmap –sX –v (alamat IP)
- FIN scan : nmap –SF (alamat IP)
- Null scan : nmap –sN (alamat IP)
- UDP Scan : nmap –sU –v (alamat IP)

Firewall IDS?

Terima Kasih

Materi Berikutnya:

Memahami hasil Scan

Keamanan Jaringan

13. Memahami hasil Scan

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Status Port

1. Open : terbuka
2. Closed : tertutup
3. Filtered : ada firewall?
4. Unfiltered : Portnya ada, open/closed? →perlu scan lanjutan
5. Open|Filtered: open/filtered? → perlu scan lanjutan
6. Closed|Filtered: closed/filtered? →perlu scan lanjutan

Port Target

- 80 : http
- 443 : https
- 53 : DNS
- 25 : SMTP
- 22 : SSH
- 23 : Telnet

- 20 & 21 : FTP
- 135-139 dan 445: Windows file sharing, login dan Remote Procedure Call
- 500 : untuk IPSEC & VPN
- 123 : NTP

Terima Kasih

Materi Berikutnya:

Vulnerability Scanning

Keamanan Jaringan

14. Vulnerability Scanning

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Vulnerability

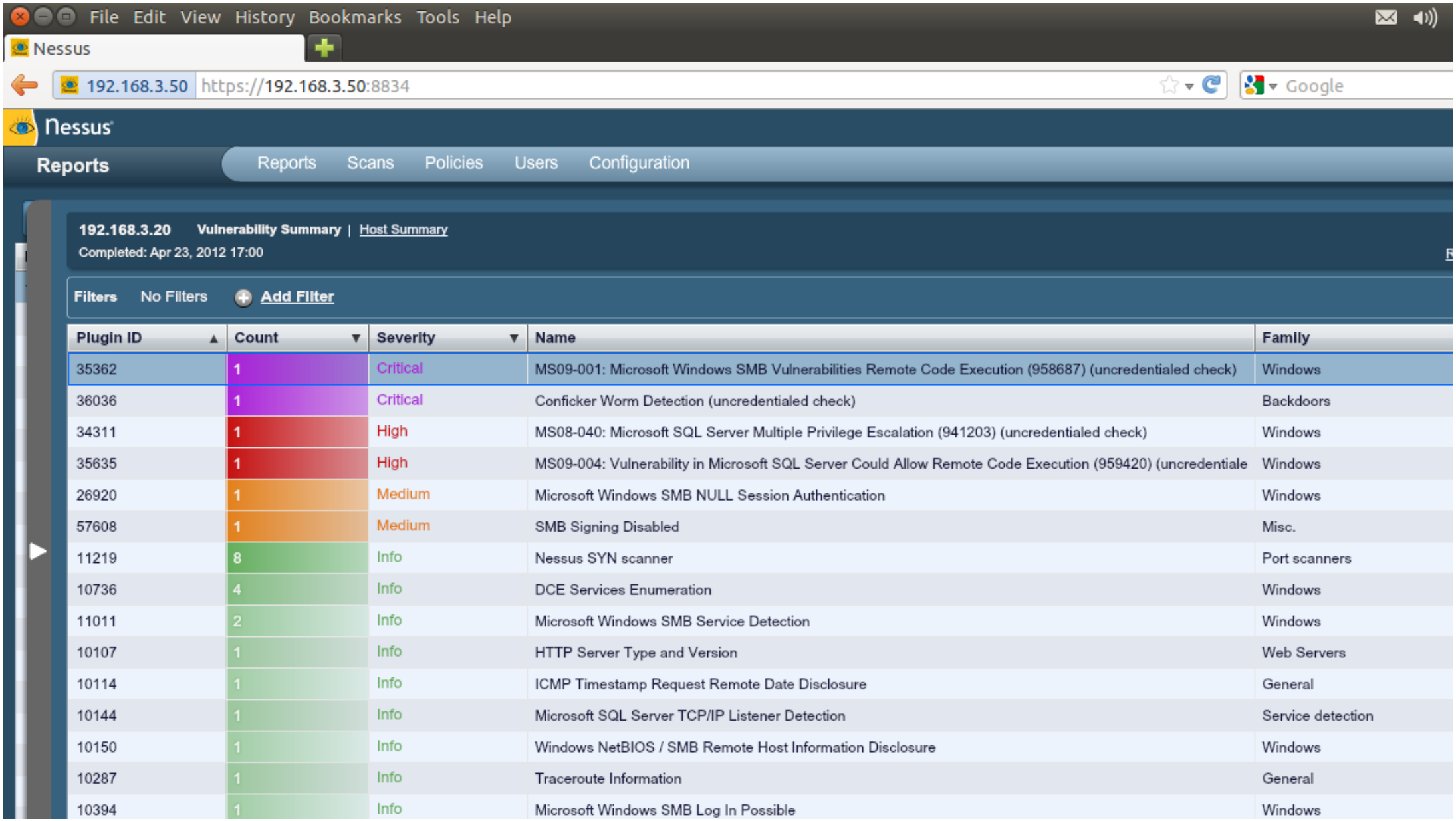
- Vulnerability = Celah keamanan
- Menentukan exploit yang digunakan
- Tingkatan Vulnerability:
  - Low
  - Medium
  - High
  - Critical

Database Celah Keamanan

- CVSS : Common Vulnerability Scoring System → www.first.org
- CVE: Common Vulnerabilities and Exposure → cve.mitre.org

Tools Vulnerability Scan

- Nessus
- OpenVAS
- Nexpose
- Retina
- GFI Languard
- Qualsys FreeScan
- dll



Plugin ID	Count	Severity	Name	Family
35362	1	Critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows
36036	1	Critical	Conficker Worm Detection (uncredentialed check)	Backdoors
34311	1	High	MS08-040: Microsoft SQL Server Multiple Privilege Escalation (941203) (uncredentialed check)	Windows
35635	1	High	MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentiale	Windows
26920	1	Medium	Microsoft Windows SMB NULL Session Authentication	Windows
57608	1	Medium	SMB Signing Disabled	Misc.
11219	8	Info	Nessus SYN scanner	Port scanners
10736	4	Info	DCE Services Enumeration	Windows
11011	2	Info	Microsoft Windows SMB Service Detection	Windows
10107	1	Info	HTTP Server Type and Version	Web Servers
10114	1	Info	ICMP Timestamp Request Remote Date Disclosure	General
10144	1	Info	Microsoft SQL Server TCP/IP Listener Detection	Service detection
10150	1	Info	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows
10287	1	Info	Traceroute Information	General
10394	1	Info	Microsoft Windows SMB Log In Possible	Windows

Terima Kasih

Materi Berikutnya:

Keamanan Password

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.