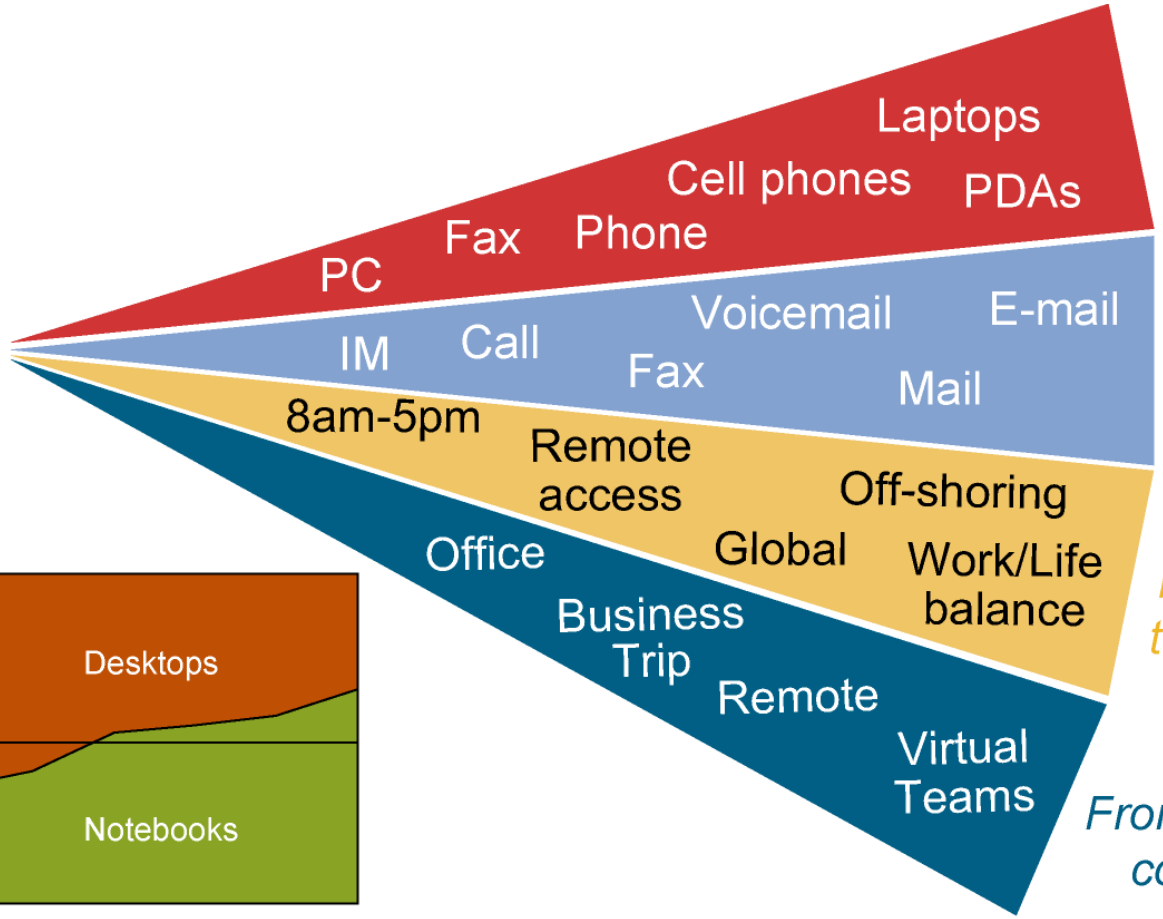
Network Security in "Wireless/Cellular" Data Communication

Josua M Sinambela, CCNP, CCNA, CEH, CompTIA Security+
RootBrain IT Security Training & Consulting
www.rootbrain.com

Pembahasan

- Trend Market Todays >> Wireless Technology
- Cellular Data Network
- Arsitektur Cellular Network
- Mitos-mitos dan Persepsi Keliru
- Network Security Investigation
- Teknologi Keamanan Jaringan "*Cellular*"
- Demo Security in Cellular Network
- Diskusi & Tanya-Jawab

Trend Market : Wireless Technology



More notebooks sold than desktops

301P_403

Cellular Data Network

- **Termasuk Teknologi *Cellular Data Network :***

» **EV-DO, Rev A, Rev 0**

» **HSDPA, HSUPA, HSPA**

» **CDMA, CDMA2000, 1xRTT**

» **GSM, EDGE, GPRS**

» **4G, 3G, 2.5G, 2G**

» **UMTS**

» **LTE**

» **WiMax**

» **Broadband**

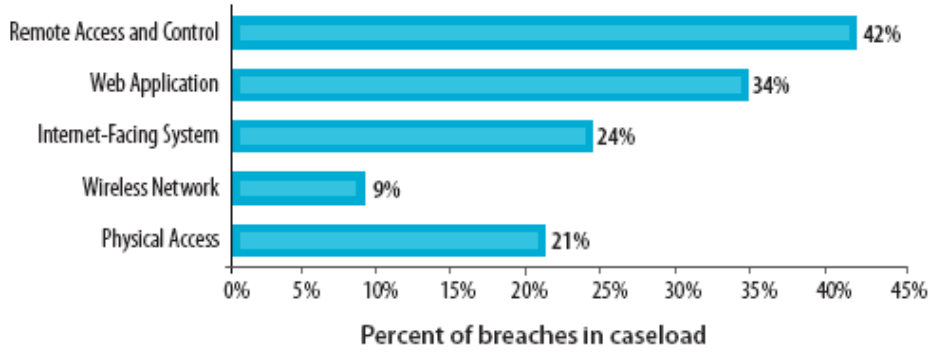
- **Speeds & coverage berbeda tergantung *carrier* & teknologi**
- **Tidak ada perbedaan berkaitan permasalahan keamanan komunikasi data**

Cellular Data

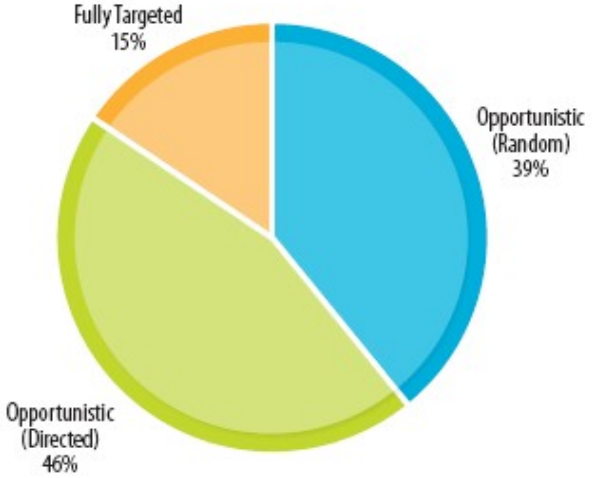
- Cellular Data = Jaringan Internet (Publik)
  - » Indosat
  - » Telkomsel
  - » Excelcomindo (XL)
  - » Three (3)
  - » AXIS.
- Umumnya Network Operator sebagai Cellular Carrier yang menjadi Internet Service Provider (ISP) memberikan link langsung ke Jaringan Publik (INTERNET)
- Di Internet terdapat berbagai ancaman Crackers/Hackers, Denial-of-Service, Viruses, Spy-Ware, Trojan, Phising, Spoofing, Sniffing dst
- Problem keamanan bertambah kompleks jika perangkat yang akan diamankan bukan hanya PC tetapi juga Camera, PLC, sensor dst.
- Menggunakan Link Data Cellular secara terbuka dan tanpa proteksi = Vurnerable = Telanjang = Menjadi target banyak *Threats*

A Verizon Research : Four Years of Forensic Research

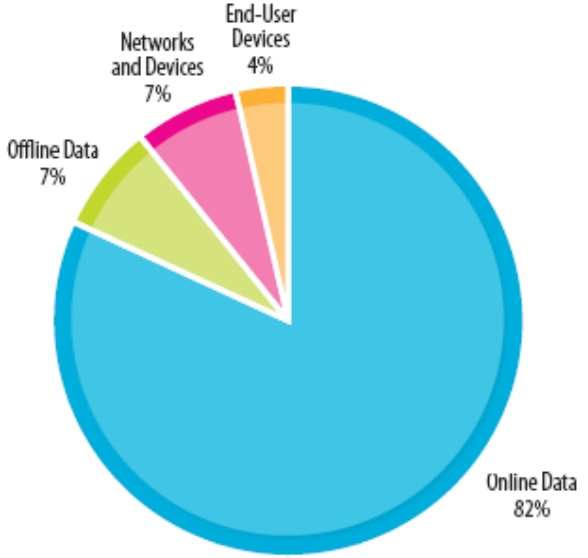
Common Attack Pathways



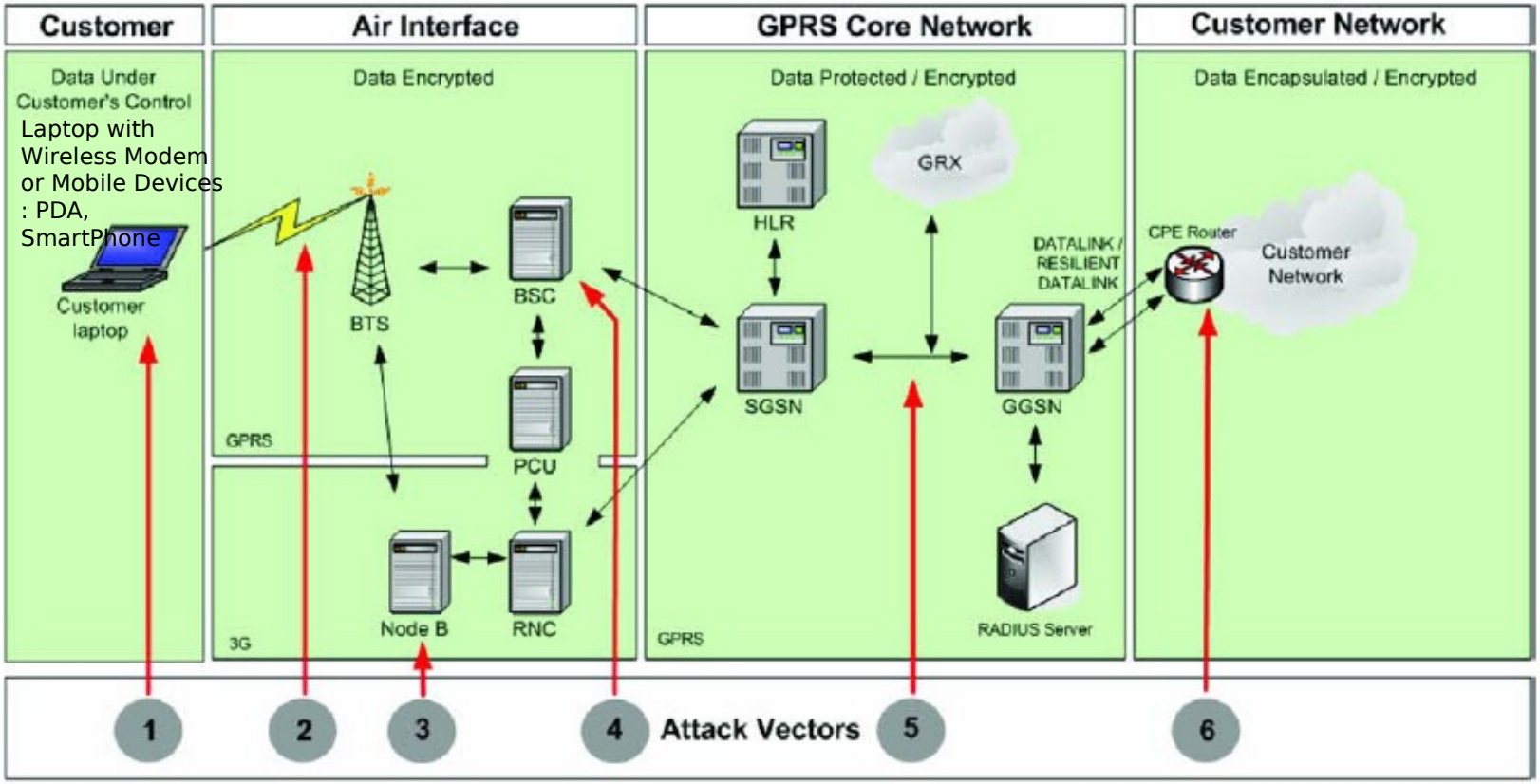
Targeted vs. Opportunistic Attacks



Compromised Assets

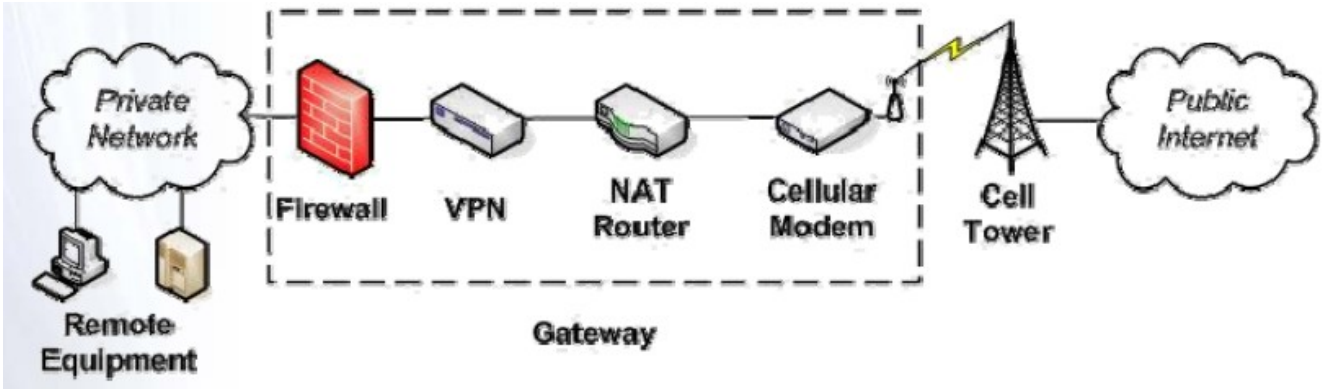


Arsitektur *Cellular Network*



Istilah keamanan yang harus di pahami

- IP Publik vs IP Private addresses
- Cellular Modem
- Router
- NAT – network address translation
- VPN – virtual private network
- Firewall
- Gateway



Mitos-mitos :

- ***"Tidak ada yang peduli dengan data saya" (merasa kurang penting)***
  - **Ada benarnya**
  - **Hacker/Cracker memang tidak selalu tertarik dengan data Anda**
  - **Tujuan mereka ingin mengontrol perangkat Anda, untuk dijadikan:**

» Zombie servers – spam - DDoS

» Back-door to corporate network

» Data loss / corruption

» Increased telecom costs

- **Koneksi yang mereka peroleh mungkin dapat/akan digunakan suatu saat nanti.**
- **Kompetitor Anda mungkin tertarik dengan data anda .. (dijual?)**

Mitos-mitos :

- *"Hackers tidak tertarik dengan perangkat wireless/cellular"*
  - **Secara umum target para cracker/hacker adalah yang memiliki "*higher value*" spt Bank-Bank atau Credit Cards**
  - **Cracker/Hackers tidak peduli apakah perangkat anda adalah wireless/cellular atau bukan.**
  - **Cracker/Hackers umumnya melakukan port scanned untuk mendapatkan kelemahan sistem/perangkat**
  - **Beberapa koneksi jaringan operator cellular bersifat terbuka, tanpa diproteksi.**
  - **Keamanan tergantung pada Anda & perangkat Anda, dan para Hacker/Cracker sangat paham hal ini.**

Mitos-mitos :

- **“*Cellular Devices (Non-PC)* dapat tahan terhadap serangan-serangan para Cracker/Hackers”**
  - ***Cellular Devices* juga menggunakan sistem operasi Embedded OS spt Windows, Linux, Windows CE, Apple & lainnya. Jadi.. tetap memiliki vulnerable spt PC/Desktop.**
  - **Banyak produk-produk *Cellular* tidak melalui proses security testing.**
  - ***Cellular devices* relatif lebih jarang dilakukan patching atau update aplikasi.**
  - **Serangan pamungkas “Denial of Services (DoS)” sangat mudah dilakukan.**

Kesalahan persepsi/konsep:

- *"Dengan NAT pasti sudah Aman"*
  - **NAT merupakan bentuk firewall yang paling fundamental.**
  - **NAT tidak cukup**
  - **NAT belum mempu mengatasi IP Spoofing**
  - **Setiap komunikasi data yang dilakukan akan membukakan sebuah atau lebih ports.**
  - **Jika ada port yang terbuka, maka Anda menjadi Vulnerable**
  - **Cara untuk mengurangi resiko ini adalah memanfaatkan Access Control List (Trusted IP)**

Kesalahan persepsi/konsep:

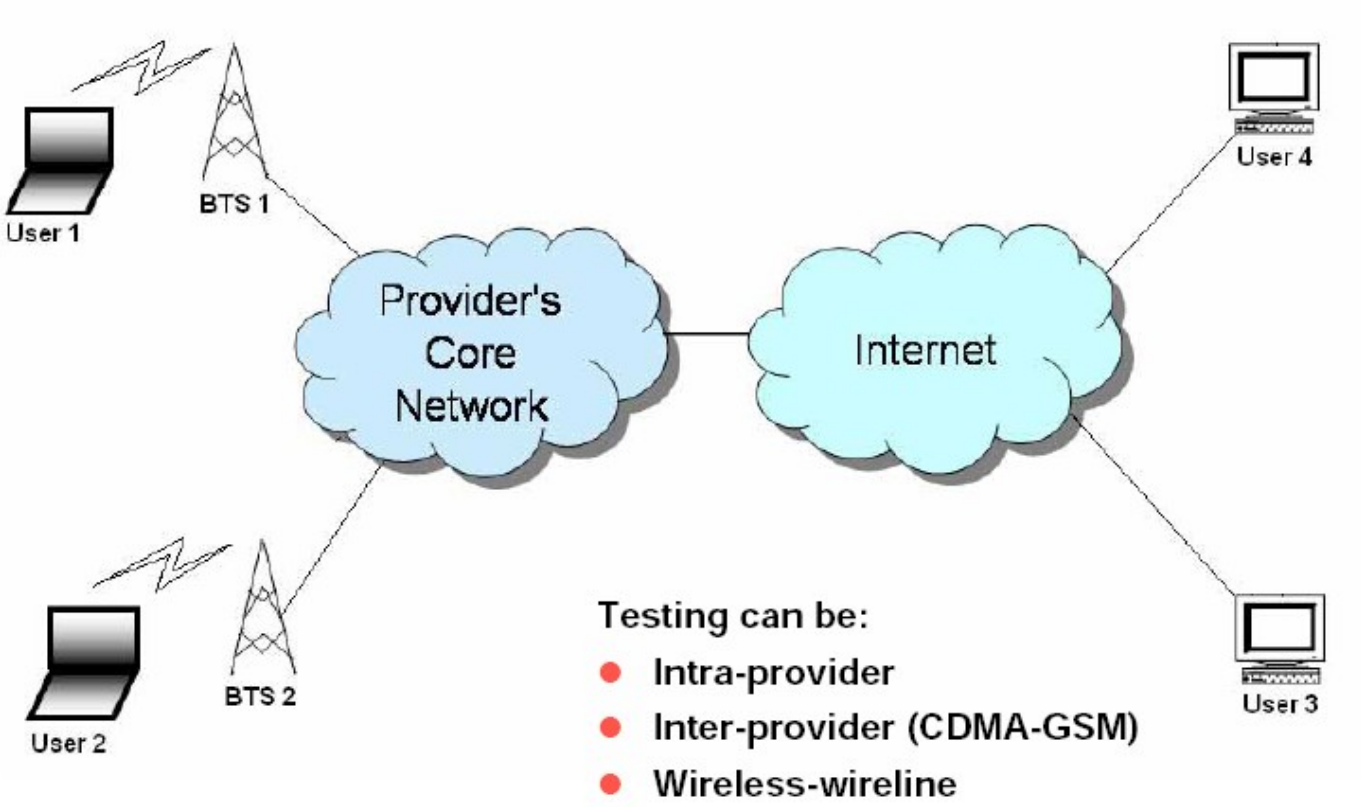
- *"Jaringan data Operator Cellular saya sudah Aman"*
  - **Jelas … pasti itu.**
    - ✓ **Radio link terenkripsi**
    - ✓ **Perangkat terhubung ada otentikasi**
    - ✓ **Ada firewall menuju internet**
  - **Security tersebut hanya mengamankan jaringan mereka, bukan perangkat Anda**
  - **Operator firewall, umumnya hanya untuk proteksi serangan dari Internet**
  - **Perangkat kita dibelakang firewall operator/provider, tidak menjamin keamanan kita. (rules dan policy bergantung operator/provider)**
  - **Koneksi pengguna Operator Celluler yang sama umumnya terbuka (dapat saling akses tanpa proteksi, Peer-to-Peer Attack)**
  - **Keamanan data harus tetap kita managed sendiri**

Kesalahan persepsi/konsep:

- *"Jaringan data Operator Cellular saya sudah aman karena menggunakan IP Private"*
  - **Secara default IP Private tidak dapat terhubung internet**
  - **Harus ada proses translasi di jaringan provider, muncul permasalahan Bandwidth dan jumlah koneksi yang terbatas akibat proses Network Translasi tersebut.**
  - **Penggunaan IP Private akan membatasi pilihan design jaringan untuk mengakses remote site.**
  - **Anda tetap Vulnerable dari pengguna lainnya yang menggunakan operator yang sama (berada pada jaringan lokal yang sama).**

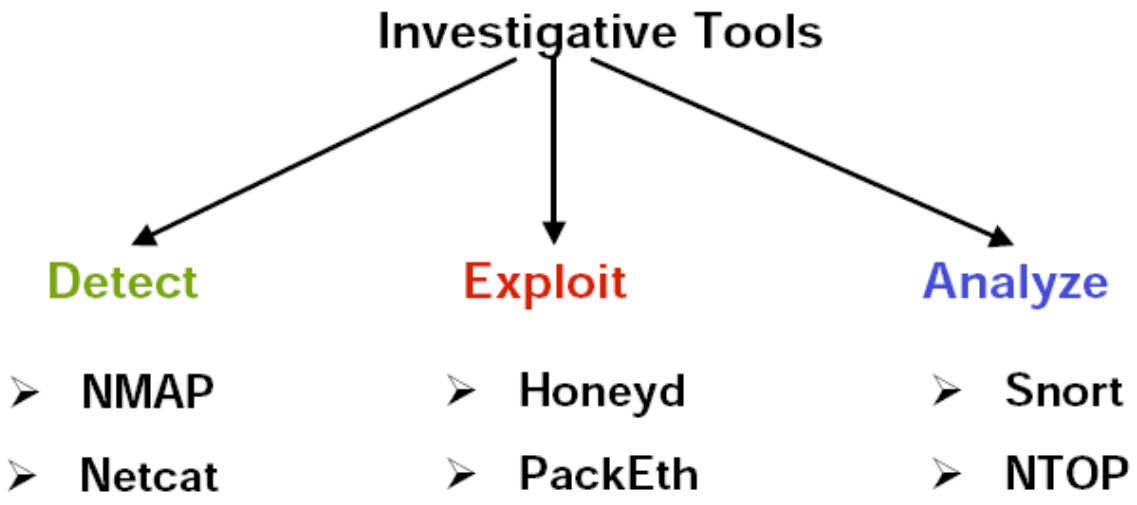
Network Security Investigation

- ***Network Security Testing***



Network Security Investigation (Cont.)

- ***Network Security Tools***



Network Security Investigation (Cont.)

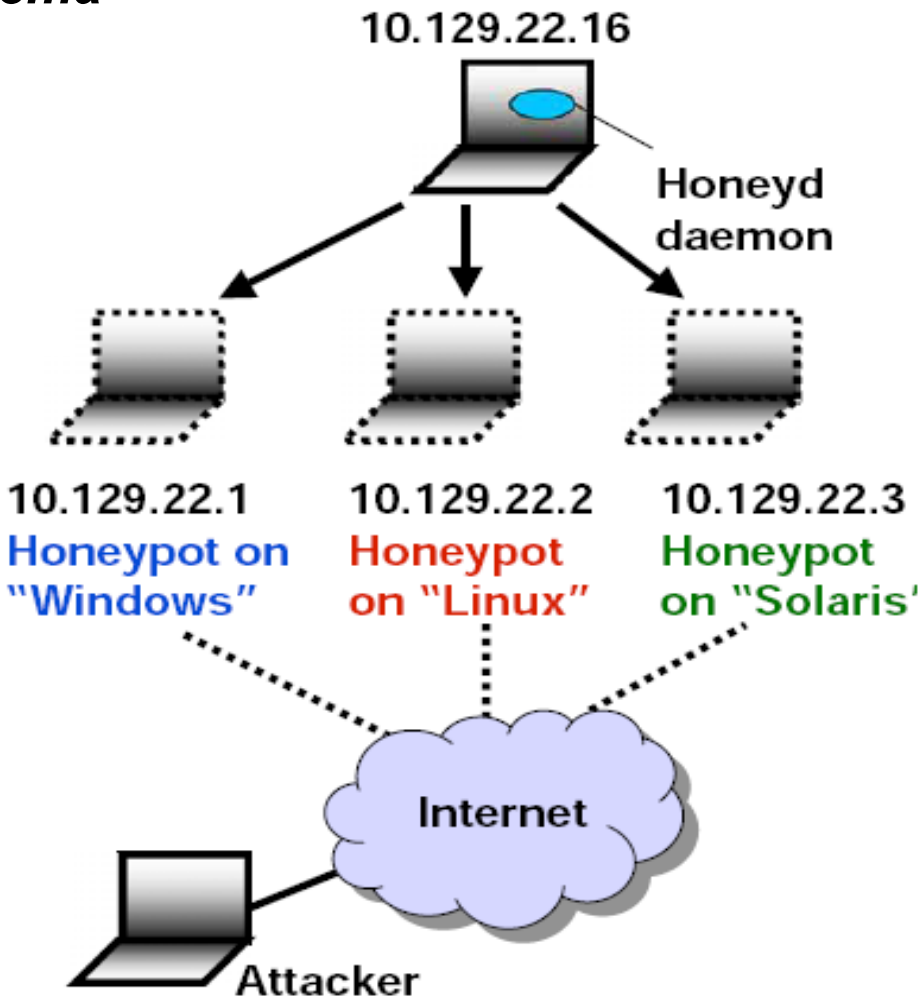
- ***Network Security Detection Tools***
  - **Network MAPper (NMAP)**
    - **Determines running apps. on target.**
    - **Identifies open ports, OS, firewalls used by remote host(s)**
  - **Netcat**
    - **Utility used to read/write across network connections using**
    - **TCP/UDP protocol(s)**
    - **Feature-rich, network debugging and exploration tool**

Network Security Investigation (Cont.)

- ***Network Security Exploitation Tools***
  - **HoneyD:**
    - **Creates virtual machines (VMs)**
    - **VMs have unique IP addresses**
    - **Lure attackers to themselves**
    - **Can be Windows or Linux**
  - **PackETH:**
    - **Packet generator**
    - **Generates packets of any protocol - ARP, TCP, UDP, ...**
    - **User configurable pkt. profiles**

Network Security Investigation (Cont.)

- ***HoneyD Skema***



Network Security Investigation (Cont.)

- ***Network Security Analyzing Tools***
  - **Snort**
    - **Real-time traffic analysis & packet logging**
    - **Usable in multiple modes:**
    - **Packet sniffer**
    - **Data logger**
    - **Intrusion detection**
    - **Generates variety of alerts – usable for proactive detection**
  - **NTOP**
    - **Traffic usage monitor & packet analyzer**
    - **Supports mgt. activities: planning, opt., detection**
    - **Tracks ongoing attacks, generates alarms**

Network Security Investigation (Cont.)

- ***SNORT in Action***

```
 GNU nano 2.0.6            File: /var/log/snort/alert

[**] [1:11267:4] WEB-CLIENT Adobe Photoshop PNG file handling stack buffer overflow atte$
[Classification: Attempted User Privilege Gain] [Priority: 1]
04/14-20:50:19.776705 70.84.240.122:80 ->              :60259
TCP TTL:44 TOS:0x0 ID:5550 IpLen:20 DgmLen:1480 DF
***A**** Seq: 0x2DE7572B  Ack: 0x9426A513  Win: 0x1920  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2365][Xref => http://www.sec$

[**] [1:486:5] ICMP Destination Unreachable Communication with Destination Host is Admin$
[Classification: Misc activity] [Priority: 3]
04/15-14:47:15.916633 202.186.153.2 ->
ICMP TTL:245 TOS:0xC0 ID:35173 IpLen:20 DgmLen:68
Type:3  Code:10  DESTINATION UNREACHABLE: ADMINISTRATIVELY PROHIBITED HOST FILTERED
** ORIGINAL DATAGRAM DUMP:
            :45290 -> 202.186.153.2:80
TCP TTL:54 TOS:0x0 ID:58279 IpLen:20 DgmLen:40 DF
Seq: 0x3038E18C
(12 more bytes of original packet)
** END OF DUMP

[**] [1:486:5] ICMP Destination Unreachable Communication with Destination Host is Admin$
[Classification: Misc activity] [Priority: 3]
04/15-14:47:16.012838 202.186.153.2 ->
ICMP TTL:245 TOS:0xC0 ID:35174 IpLen:20 DgmLen:68
Type:3  Code:10  DESTINATION UNREACHABLE: ADMINISTRATIVELY PROHIBITED HOST FILTERED
** ORIGINAL DATAGRAM DUMP:
            :45291 -> 202.186.153.2:80
TCP TTL:54 TOS:0x0 ID:56305 IpLen:20 DgmLen:40 DF
Seq: 0x3906E8D7
(12 more bytes of original packet)
```

Basic Analysis and Security Engine (BASE)

Home | Search

Queried on : Tue April 15, 2008 15:56:55

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Summar
- Sensor
- Unique
- (clas
- Unique
- Unique
- Source
- Destina
- Time p

Displaying alerts 1-48 of 154 total

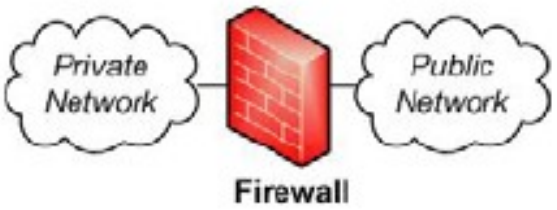
ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-1)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:15	202.186.153.2		ICMP
#1-(1-2)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:16	202.186.153.2		ICMP
#2-(1-3)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:16	202.186.153.2		ICMP
#3-(1-4)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:16	202.186.153.2		ICMP
#4-(1-5)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:16	202.186.153.2		ICMP
#5-(1-6)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:16	202.186.153.2		ICMP
#6-(1-7)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2008-04-15 14:47:17	202.186.153.2		ICMP

Teknologi Keamanan Jaringan "*Cellular*"

- NAT & Firewalls
- VPN & Encryption
- Remote Monitoring & Alerts
- Modems vs. Gateways

NAT & Firewall

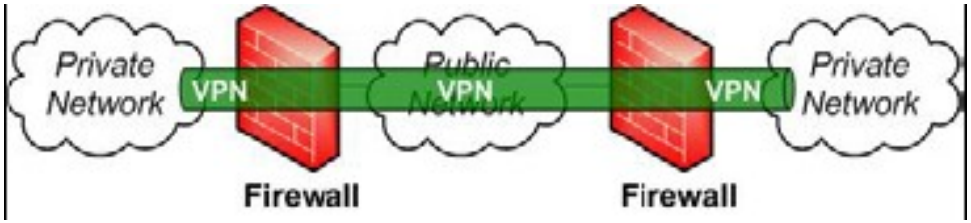
- NAT is a basic type of firewall – no granular control
- Stateful Packet Inspection Firewalls
  - *Pass/Reject Rules & Filters:*
    - By Port
    - By Protocol & Packet Type
    - By Source / Destination IP
    - By Time of Day



- Rules sets for every packet direction
- Anti-probing & denial-of-service protection
- Alerting & Logging

VPN & Encryption

- Most secure communication option
- IPSec, PPTP, L2TP, GRE
- Site-to-Site
- Client-to-Site



- Hardware vs. Software VPN
- Pre-shared Keys vs. Digital Certificates
- Encryption – DES, 3DES, AES
- Performance issues

Remote Monitoring & Alert

- Proactive notification of security events
  - Unauthorized access attempts
  - Configuration changes
  - Port scans
  - Service attacks
- Syslog Server
- Central Management Console
- E-Mail / Pager
- SNMP traps

Modem vs Gateway

- **Modem = Koneksi Internet Tanpa Proteksi**
  - **Umumnya pengguna hanya menggunakan Modem untuk terhubung Internet**
  - **Koneksi Cellular dengan Modem dapat berupa PC/Laptop dengan External Modem (3G/HSDPA/GPRS/USB) atau menggunakan Internal Modem (Embedded) seperti SmartPhone/PDA/Iphone/Notebook Builtin 3G Modem**
  - **Pada perangkat dengan Embedded Modem, relatif akan lebih sulit dilakukan pengamanan.**
  - **Untuk keamanan terbaik idealnya, modem dikombinasikan dengan NAT Router, Firewall, VPN dan Remote Monitoring.**
  - **Kombinasi ini yang biasa disebut sebagai "Gateway"**

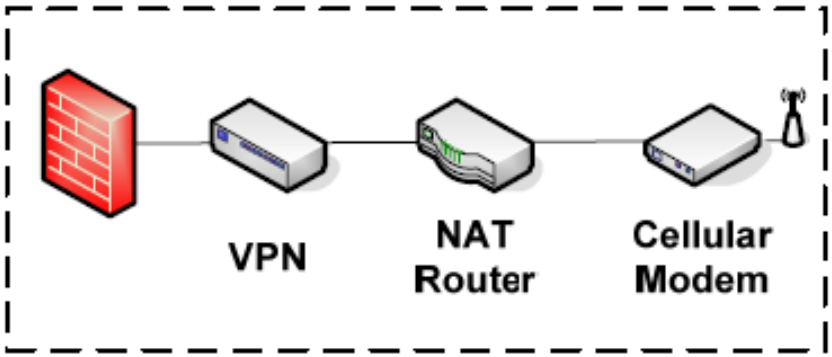




Modem vs Gateway

Gateway = Secure Internet access via 1 device

- Modem +
  - *Firewall*
  - *VPN & Encryption*
  - *NAT Routing & Port Forwarding*
  - *Event monitoring & alerting*



Demo

- Koneksi menggunakan GPRS/3G/UMTS/HSDPA
- Koneksi dari/ke sesama Operator Cellular
- Koneksi dari/ke berbeda Operator Cellular
- Koneksi dari Internet ke Perangkat Celluler
- Enumeration & Scanning
- Remote Exploitation

Selesai… Terimakasih

Sesi Diskusi & Tanya jawab..