

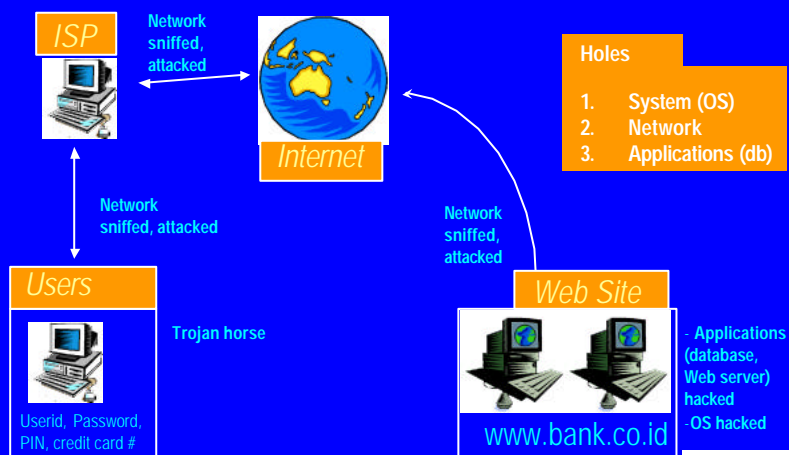
Overview of Network Security

Budi Rahardjo
budi@indocisc.com
<http://budi.insan.co.id>

net security - budi rahardjo



Security Holes



net security - budi rahardjo



Focus on this presentation

NETWORK SECURITY

net security - budi rahardjo



Types of network attack

- Interruption
 - DoS attack, network flooding
- Interception
 - Sniffed (password)
- Modification
 - Trojan horse
- Fabrication
 - Spoofed packets

net security - budi rahardjo



Reality Check

- IP v.4 is unsecure. Spoofing is easy
- Tools (scripts) to exploit are available
- More home users are connected 24 hours/day with DSL, cable modem
- Need collaboration among network providers
 - Ingres filter @ border routers

net security - budi rahardjo



Interruption Attack

- Denial of Service (DoS) attack
 - Exhaust bandwidth, network flooding
 - Possible to spoofed originating address
 - Tools: ping broadcast, smurf, synk4, various flood utilities
- Protection:
 - Little we can do if we are under attacked
 - Filter at router for outgoing packet, filter attack originating from our site

net security - budi rahardjo



More interruption attack

- Distributed Denial of Service (DDoS) attack
 - Flood your network with spoofed packets from many sources
 - Based on SubSeven trojan, “phone home” via IRC once installed on a machine. Attacker knows how many agents ready to attack.
 - Then, ready to exhaust your bandwidth
 - See Steve Gibson’s paper <http://grc.com>

net security - budi rahardjo



Interception Attack

- Sniffer to capture password and other sensitive information
- Tools: tcpdump, ngrep, linux sniffer, dsniff, trojan (BO, Netbus, Subseven)
- Protection: segmentation, switched hub

net security - budi rahardjo



Modification Attack

- Modify, change information/programs
- Examples: Virus, Trojan, attached with email or web sites
- Protection: anti virus, filter at mail server, integrity checker (eg. tripwire)

net security - budi rahardjo



Fabrication Attack

- Spoofing address is easy
- Examples:
 - Fake mails, spoofed packets
- Tools: various packet construction kit
- Protection: filter outgoing packets at router

net security - budi rahardjo



Protection

- Firewall
 - Static vs Stateful Packet Filter
 - Circuit gateway, application level gateway
- Intrusion Detection System (IDS)
 - Host vs Network based
- Policy
 - Privacy issues, AUP, cyberlaw, best practice, what to do if your site is probed?

net security - budi rahardjo



Firewall – Static Packet Filter

- Inspect packets based on rules
 - Source, destination address, port
- Strength:
 - fast, can be implemented with Linux box
- Weakness: can be fooled, changing order, fragmentation, little information (for logging), IP spoofing, does not inspect payload, difficult to configure (lots of rules), stateless

net security - budi rahardjo



Firewall - Stateful

- Remembers the state of packets
- Strength: better inspection, can be implemented with Linux box
- Weaknesses: slower?/faster?, needs more resources, IP spoofing, does not inspect payload, still difficult to configure

net security - budi rahardjo



Intrusion Detection System

- Monitor system for anomaly
- Monitor host or network? Hybrid
- Difficult to monitor if stealth and slow
- Tools example: snort

net security - budi rahardjo



Policy

- The hardest thing to do is dealing with people
- Policy, Standard Operating Procedure is overlooked

net security - budi rahardjo



More reading materials

- My Books: Handbook Security
<http://budi.insan.co.id>
- Security focus <http://www.securityfocus.com>
- Packetstorm <http://www.packetstormsecurity.org>
- Securiteam <http://www.securiteam.com>
- Security Tracker <http://www.securitytracker.com>
- and many more ...

net security - budi rahardjo

