Internet infrastructure

Prof. dr. ir. André Mariën
Topic

Firewalls

(c) A. Mariën
31/01/2006
Firewalls

• Only a short introduction
• See for instance:
  – Troubleshooting linux firewalls, M. Shinn, S. Shinn, addison wesley
  – Linux firewalls (attack detection and response with iptables, psad and fwsnort), M. Rash, no starch press
Requirements

– RFC 2979: Behavior of and Requirements for Internet Firewalls
  • Firewalls either act
    – as a protocol end point and relay
    – as a packet filter
    – some combination of both

– Firewall as a protocol end point
  • implement a "safe" subset of the protocol
  • perform extensive protocol validity checks
  • use an implementation methodology designed to minimize the likelihood of bugs
  • run in an insulated, "safe" environment
  • use some combination of these techniques in tandem

– Firewalls acting as packet filters aren't visible as protocol end points. The firewall examines each packet and then
  • passes the packet through to the other side unchanged
  • drops the packet entirely
  • handles the packet itself in some way.
What does a Firewall do?

• Focus for security decisions
• Enforce security policy
• Log activities
• Limit exposure
What does a Firewall not do?

- Protect against insiders
- Protect connections it does not see
- Protect against day-zero attacks
- Protect against all viruses
- Configure itself automatically
Attacks

• Attack types
  – Intrusions
  – Denial of Service (DoS)
  – Information theft

• Attacks: examples
  – Port scanning
  – IP spoofing
  – IP based DoS
Security principles

- Least privilege
- Defense in depth
- Choke point
- Weakest link
- Fail-safe
- Diversity of defense
- Simplicity
Technologies

• Packet filtering
  – Allow protocols and services
  – Allow connections in defined directions

• Proxy services
  – Proxies provide choke point
  – Proxies enforce policies
Technologies (cont.)

• Network Address Translation (NAT)
  – Information hiding
  – De-facto blocking (non-routable addresses)

• Virtual Private Networks (VPN)
  – Support for extranets
NAT & filtering in IP tables

Application socket

Filter INPUT

Filter OUTPUT

NAT prerouting

route

Filter FORWARD

NAT postrouting
IP tables filter definitions

• Filters:
  – Source
  – Destination
  – State
  – Protocol
  – Content
  – MAC

• Action
  – ACCEPT
  – DROP
  – LOG
  – RETURN
Proxy usage

- Proxies require proxy-aware application software
- Proxy-aware OS software
  - OS libraries
  - JVM
- Proxy-aware router
  - transparent proxy
Proxy types

- Application level proxy
- Circuit level proxy
Proxy operation: 2 connections
Proxy operation: client aware

GET /index.htm

GET http://server/index.htm

GET /index.htm
Transparent proxy

• Proxy system behaves as a router
• Transparently passes requests through a proxy service
• Configuration: as if a direct connection with the Internet is possible
• Mind IP addresses INSIDE the protocol
Proxy FTP

• Access style one:
  – ftp proxy
  – User: userID@targetFTPserver
  – ...

• Alternative
  – ftp proxy
    • Optionally, proxy authentication: User & password
  – OPEN targetFTPserver
  – ...

(c) A. Mariën
Proxy authentication HTTP

• Authentication to “get out”

• HTTP proxy authentication
  – HTTP proxy sends reply: 407 (proxy authentication required)
  – Client
    • Prompts user for UID/password
    • sends Proxy-Authorization header back with repeated request
Proxy authentication: scheme

Proxy authentication: “Proxy-authorization: xy65f”

Server authentication: “Authorization: DFER5SD”
Caching proxy

- Proxy is central point of access
- Caching at this point very interesting
- Typically some active subset exists
- Need to address unwanted caching in applications (inter-user contamination)
Common firewall types

• Single box
  – screening router
  – dual homed host

• Screened host
  – screening router + host

• Screened subnet
  – exterior router + LAN + hosts + interior router
Bastion host hardening

• secure the machine
  – use checklist and scripts
• disable non-required services
  – enable only required services
• enable auditing
• provide secured access for management (SSH)
• run security audit

• See also:
  – http://checklists.nist.gov/
  – http://www.sans.org/reading_room/whitepapers/linux/
Firewalls in infrastructure
Infrastructure goal: zones

• basic: two zones
  – internet
  – intranet

• simple: three zones
  – internet
  – De-Militarized Zone: DMZ
  – intranet
Two zones, one firewall

internet

---

intranet

internet

intranet

(c) A. Mariën

31/01/2006
Two zones, one firewall

• firewall does everything:
  – filters traffic
  – does NAT
  – runs proxies

• single point of failure

• most basic set-up:
  – “firewall” is actually screening router:
More realistic
Three zones, one firewall

internet

DMZ

intranet

internet

DMZ

intranet
Three zones, two firewalls
More realistic

internet

DMZ

intranet

internet

Router

Firewall

switch

Firewall

HUB

internet

Router

Firewall

switch

Router

HUB

(c) A. Mariën