Network defenses
firewalls

Thanks to Tom Dunigan @ UTK
In the news

• Man draws 10 yr sentence for sending trojans, blackmailing minors
• Denial of service now punishable by 10 yr sentence in UK
• Phishers spoofing Social Security Administration
• Judge shuts down spyware and malware purveyors
Network defenses

- disable
- configure properly
- xinetd, tcpwrappers
  - filters (allow, deny)
  - audit and alarm
- filtering portmap
- application filtering (securelib)
- patches
- scanners (Nessus, SATAN, ISS)
- firewalls
- intusion detection & response
- encryption, IPsec, virtual private networks (VPNs)

Defense in depth

- on a hill
- moat
- outer wall
- archer towers
- inner wall
Assess your attack surface

Scanners
  ISS, Nessus, nmap -- probe and report network hosts and services

- point, click, scan a net
- port probes (nmap)
- OS type probes (nmap)
- portmap probes
- X and NFS attempts
- sendmail checks
- NIS probes
Network countermeasures

- host-based (wrappers, personal firewalls)
- router based (filters)
- firewalls
- Intrusion Detection Systems (IDS/IPS)
- authentication/encryption (IPsec/VPNs)
Host network services “wrappers”

• network/host access control lists
• re-write applications with filters (securelib)
• replace inetd with filtering version (xinetd)
• use tcp wrappers
  – free, no changes to application
  – inetd services only
  – allow/deny
  – double DNS lookups
  – audit and alarm
  – API for new app’s

/etc/inetd.conf
ftp    stream  tcp     nowait  root /usr/sbin/tcpd  wu.ftpd
telnet  stream  tcp     nowait  root /usr/sbin/tcpd  in.telnetd
shell   stream  tcp     nowait  root /usr/sbin/tcpd  in.rshd -l
login   stream  tcp     nowait  root /usr/sbin/tcpd  in.rlogind

/etc/hosts.deny
in.rlogind: ALL
in.telnetd: ALL
in.rshd: ALL
wu.ftpd: ALL

/etc/hosts.allow
in.rlogind: 128.219., 134.167., 127.
in.telnetd: 128.219., 134.167., 127.
in.rshd: 128.219., 134.167.
firewalls

- NO connection -- best 😊
- toolkits, personal firewalls (Linux, PC)
- filtering/screening routers
- dual-homed gateways (bastion host)
- screened host gateway
- screened subnet (NAT)
- commercial solutions (enterprise firewalls)
Personal (host) firewalls

- Network access control lists
  - Which hosts/nets you permit/deny
  - Which services you permit/deny
  - Make your host invisible to net (ping/port scans)
- PC/Windows – XP firewall (ICF), ZoneAlarm, NetIce
- Linux – iptables
- MAC – ipfw

Difficult to configure and EVERY host needs to do it.
If bad guy gets in to your host, he’ll disable your host’s firewall.
Windows firewall

- Security Center (firewall, auto updates, viruses)
  - Blocks outside requests
  - Alerts if program attempts to use Internet
  - Add exceptions (program or port)
  - Keeps a log
**ZoneAlarm Alert**

**New Program**

Do you want to allow netforum.exe to access the Internet?

**Technical Information**

Destination IP: 210.80.59.34 DNS
Application: netforum.exe
Version:

**More Information Available**

This is the program's first attempt to access the Internet.

**AlertAdvisor**

Remember this answer the next time I use this

([Select] Yes [Select] No)

---

**ZoneAlarm Alert**

**Protected**

The firewall has blocked Internet access to your computer (NetMeeting) from 204.1.226.226

(NetMeeting Name)

Time: 03/03/2004 8:14:46 AM

**AlertAdvisor**

Don't show this dialog again

([Select] Yes [Select] No)

---

**Programs**

<table>
<thead>
<tr>
<th>Program</th>
<th>Access</th>
<th>Trusted</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe &amp; Internet Update</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application Layer Gateway Service</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>AvastMail - Mail manager, AntiSpam, sends reply message</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Generic Host Process for Win32 Services</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Messenger</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Mozilla</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Outlook Express</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Services and Controller app</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Spybot - Search &amp; Destroy</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Windows Service Pack Setup</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Zone Labs Client</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Linux firewalls

- ipfwadm begat ipchains begat iptables
- accept/reject rules (tables) + logging
- RedHat select security (high, medium, none)
- provides Network Address Translation (NAT), masquerading
  - IPforwarding (private nets 10.0.0.0, 172.16.0.0, 192.168.0.0)

```
iptables -F iptables -A INPUT -i lo -p all -j ACCEPT - Allow self access by loopback interface
iptables -A OUTPUT -o lo -p all -j ACCEPT
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT - Accept established connections
iptables -A INPUT -p tcp --tcp-option ! 2 -j REJECT --reject-with tcp-reset iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT - Open ftp port
iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT - Open secure shell port
iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT - Open HTTP port
iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --syn -s 192.168.10.0/24 --destination-port 139 -j ACCEPT - Accept local network Samba connection
iptables -A INPUT -p tcp --syn -s trancas --destination-port 139 -j ACCEPT
iptables -P INPUT DROP - Drop all other connection attempts. Only connections defined above are allowed.
```
Home protection

• Personal PC firewalls (ZoneAlarm, iptables)
  – Inexpensive router, NAT, firewall
  – Home network with perimeter protection

• Wireless
  – Enable WPA key
  – Accept only designated ether addresses (MAC filter)
  – Disable SSID broadcast
  – Use ssh or VPN

• Review logs
Screening routers

- router's job is to forward packets (fast)
- add filters (ACL's) for each interface
- can block IP address spoofing of internal addresses
- should permit out only legit. local addresses
- may deny/restrict specific services (ports)

weaknesses
- complicated filter expressions
- may fail to the open mode
- limited logging
- no authentication
- DNS spoofing

Port deny list:
portmap, tftp, snmp, syslog, telnet
Restrict http to designated servers
Screening routers -- rules

! access list 102 specifies what addresses are allowed out
access-list 102 deny ip 128.219.250.0 0.0.1.255 0.0.0.0 255.255.255.255
! no snmp out
access-list 102 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 162
access-list 102 permit ip 128.219.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 102 permit ip 134.167.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 102 permit ip 192.12.68.0 0.0.0.255 0.0.0.0 255.255.255.255

! access list 112 denies local addresses from the outside
access-list 112 deny ip 128.219.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 112 deny ip 134.167.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 112 deny ip 192.12.68.0 0.0.0.255 0.0.0.0 255.255.255.255
! block a known bad guy
access-list 112 deny ip 130.225.220.16 0.0.0.0 0.0.0.0 255.255.255.255
! deny remote SNMP's and tftp's
access-list 112 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 161
access-list 112 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 69
! special internal hosts
access-list 112 deny ip 0.0.0.0 255.255.255.255 128.219.250.0 0.0.1.255

other rules for what routes are advertised
Bastion host

dual-homed (hardened) gateway

- host with two network interfaces
- IP forwarding disabled
- reachable from either side, but packets do not flow from one side to the other
- user must login to bastion host, then to other side
- supplement with application gateway software (email, ssh)
- strong authentication (Securid), logging (hardened host)
- limited services (restricted shell), wrappers
- custom mail programs
- hides enterprise network (private IP addresses)
Screened host

- common implementation
- traffic to/from Internet allowed only to bastion host, though can let internal hosts access some Internet services (ssh, ftp, www)
- bastion host acts as application gateway

Screened subnet (DMZ)

- two screening routers
- one or more bastion hosts on subnet
- internal net can be private (invisible), network
- address translation (NAT)
- place some servers on DMZ (www, anon ftp)
- place intrusion detectors, traps on DMZ
- place external DNS on DMZ
Application gateways

proxy services on the bastion host

• run minimal services (trusted OS?)
• no compilers, linkers
• use wrappers
• no local logins
• custom servers (minimal pkt forwarders, logging, ACLs)
• connections from outside
  – strong authentication (skey, securID)
  – encrypted (ssh, stel)
  – user then connects to internal host and logs in again
• 2-part mail forwarder/scanner (IPS)
  – Remove evil attachments
  – Block spam
Proxy servers

internal hosts accessing the outside (‘‘relay’’)

• need socks-ified local applications
  #define connect Sconnect
• proxy on bastion host (tn-gw, rlogin-gw, ftp-gw, x-gw, http-gw)
• servers are simple packet forwarders with ACL, e.g., telnet and an itelnet
• some services support proxies (netscape, gopher)
• socks library for building your own local apps
Enterprise firewalls

**router with an attitude**
- establish a perimeter
- single point of protection (rather than host by host)
  - Controls inbound and outbound network flows (by hosts/service)
  - logs
- principle of layering, reference monitor
  - always invoked
  - tamper resistant
  - small and simple (understandable)

**establish a policy**
- What's not denied is allowed
- What's not allowed is denied -- best
- Complicated rules

security vs convenience

---

Enclaves
use firewalls and VLANs to create internal protected subnets (e.g., business subnet, medical subnet,)

---

[Diagram showing internet, firewall, and your network]
Firewall limitations

What they don't do?
• don't do UDP very well
• don't prevent session hijacking
• don't provide privacy
• don't protect against viruses
• don't protect against insider (need internal firewalls/enclaves)
• don't prevent backdoors (modems, VPNs/tunnels)
• don't log/alarm like an IDS – some do
• don't improve throughput!

Watch out for tunneling through “permitted” ports (trojan horse)
Selecting an enterprise firewall

- commercial, consultant, kit
- filters for both in and out
- filter granularity (stateful, ftp support)
- IP fragment management
- filter language and user interface
- proxy applications, clients, extensible
- authentication mechanisms
- network address translation (NAT) and VPN
- integration with intrusion detection (IPS)
- IPv6
- logging and audit tools
- ease of install and use
- performance
- cost
Flow characterization

Firewalls allow only certain services to flow. Hackers often will trojan an allowed service, e.g., use port 80 to carry ssh traffic.

Two flows from a compromised host
Can you characterize a flow (mail, telnet/ssh, www, chat) based on flow stats (interarrival rate, packet size, volume, duration)?
Backtracking spoofed IP address flows

• Spoofed IP source addresses used by Denial of Service and session hijacking
• Perimeter routers SHOULD block spoofed addresses
  – Don’t allow internal addresses as source address from external interfaces
  – Only allow packets with valid source addresses out
• For an active attack that is using spoofed IP source addresses
  – Manually check each router along the flow, backtracking
  – Automated program to access routers and backtrack flow and setting filter to block
  – Hard: crosses administrative domains
• Other approaches, marking packets, new ICMP ... open research
High speed IDS (10-100gbs)