Bypassing Firewall

Presented by
Ricky Lou
Zecure Lab Limited

@ PISA AGM Theme Seminar 2005

Firewall Piercing (Inside-Out Attacks)

Disclaimer

We hereby disclaim all responsibility for the following hacks. If it backfires on you in any way whatsoever, that’s the breaks. Not our fault. If you don’t understand the risks inherent in doing this, don’t do it. If you use the hacks and it allow vicious vandals to break into your company’s computers and costs you your job and your company millions of dollars. Don’t come crying to us.

Firewall Piercing (Inside-Out Attacks)

Moral

A firewall cannot protect a network against its own internal users, and should not even try to.

Firewall Piercing (Inside-Out Attacks)

Inside-Out attacks try to initiate network connections from the trusted (corporate) to the un-trusted (Internet) network.

Synonym

- Inside-Out Network subversion
- Inside-Out Attack
- Covert Channel Attack

Firewall Piercing (Inside-Out Attacks)

A Covert Channel is a communication channel that allows a process to transfer information in a manner that violates the system’s security policy; without alerting any firewalls and IDS’s on the network.

The technique derives its stealthy nature by virtue of the fact that it sends traffic through ports that most firewalls will permit through.

Firewall Piercing (Inside-Out Attacks)

Direct Tunnels (Simple)

- ACK tunnel
- TCP tunnel (pop, telnet, ssh)
- UDP tunnel (syslog, snmp)
- ICMP tunnel
- IPSEC, PPTP

Firewall Piercing (Inside-Out Attacks)

Proxified Tunnels (Advance)

- □ Socks SSL tunnel
- □ HTTP/S tunnel (payload of http = tunnel)
- □ HTTP/S proxy CONNECT method tunnel
- □ DNS tunnel
- □ FTP tunnel
- □ Mail tunnel; http://www.detached.net/mailtunnel/
- □ MSN tunnel; http://gray-world.net/pr_msnshell.shtml

Firewall Piercing (Inside-Out Attacks)

Ethernet Bridging over TCP/UDP (Advance and Bloody)

- Layer 3 data (eg. IP, IPX, AppleTalk) can be encapsulated, encrypted and tunneled through Layer 4 protocol (TCP/UDP)
- Can run arbitrary any kind of TCP/IP applications behind a restrictive firewall
- Original IP address could be changed making it more stealthy
- Open VPN; http://openvpn.net/
- Implementation: http://www.ZecureLab.com

Example of Covert Channel Attacks

Netcat

- http://netcat.sourceforge.net
- very good for building reverse tunnel (i.e. Information flow through the other ways)

Example of Covert Channel Attacks

DNS Tunnel

- domain name lookup is allowed by any internal client

Example of Covert Channel Attacks

SSH Tunnel (Simple)

- TCP/IP Gender Changer
- Requires SSH port allowed by firewall

Example of Covert Channel Attacks

SSH Tunnel (Advanced)

- □ TCP/IP Gender Changer
- □ SSH over SSL Connect
- □ HTTPS Proxy Connect-Method
- □ Requires HTTPS allowed for any destinations
- □ http://gray-world.net/pr_firepass.shtml
- □ http://bypass.cc

Comment

- □ content-Filter does not help (SSL)

Example of Covert Channel Attacks

HTTP/S Tunnel

- Using POST requests
- Implementing “own” service POST requests
- POST data are in binary form

Implementations

- http://www.nocrew.org/software/httptunnel.html
- http://entreelibre.com/cctt/index_en.html

Example of Covert Channel Attacks

ICMP Tunnel

- Reliably tunnel TCP connections to a remote host using ICMP echo request and reply packets.

Implementations

- http://www.cs.uit.no/~daniels/PingTunnel/
- http://www.securiteam.com/tools/5PP0M0K60O.html
- http://www.bo2k.com/

Example of Covert Channel Attacks

Ethernet Bridging over TCP/UDP

- Reliably tunnel any network protocol (e.g. IP, IPX, AppleTalk) connections to a remote gateway using any TCP/UDP packets.
- This demonstration concentrates on IP only.
- A new identity (IP address) will be assigned.
- A new default gateway, DNS entry will be acquired.
- Your corporate LANs and the remote LANs are now unify.

Example of Covert Channel Attacks

Ethernet Bridging over TCP/UDP (con’t)

- Implications
  - More stealthy
  - Hard to trace
  - Location-tracking
  - Hide BT Traffic (seed)
  - Privacy and freedom online
  - Anonymous Surfing
  - Identity Protection

Firewall Piercing (Inside-Out Attacks)

Mitigation

- Un-plug your network cables
- Firewall: deny “any to any rules”
- Content-Filter http traffic: deny unwanted content-type
- Firewall: restrict http/s locations
- Firewall: restrict ipsec locations
- Content-filter: deny anonymizer websites

Firewall Piercing (Inside-Out Attacks)

White-listing vs. Black-listing

- Listing of the allowed resources = white-listing
- Listing of the denied resources = black-listing
- White-listing is more secure
- Black-listing is easier to handle (convenience)

Contact

E-mail

- RickyLou@ZecureLab.com

MSN

- RickyLou@RickyLou.com