OISSG

Firewall Security Assessment

Balwant Rathore, CISSP

www.oissg.org

Index

- What is Firewall ?
- Why Firewall ?
- Types of Firewall
- What a firewall cannot protect?
- How firewalls works?
- Logging
- Bypassing Firewalls
  - Mapping Firewall Rule-Base: Firewalking
  - Covert Channel

What is a Firewall?

- A hardware / software solution which ‘sits’ in between two networks, separating them and ensuring controlled access between the networks

Why Firewall?

- Reduces risk by protecting systems from attempt to exploit vulnerabilities
- Increases privacy – makes it harder to gather intelligence about your network
- Enforces your organisation's security policy

Types of Firewall

- Packet filters
- Stateful firewalls
- Application proxy
- Firewall appliance
- Stealth firewall

Packet filters

- Filters traffic based on IP address and port number
- Basic level of security
- Data contents passed through unchecked
- Example: IP Chains, Router ACLs

Stateful Firewalls

- Maintains state of each connection
- Two major implementations
  - Cut through proxy – Cisco PIX
  - State inspection – Checkpoint FW1

Stateful Inspections

- Checkpoint FW1
  - Application derived state
    - the state information derived from other applications
  - Communication derived state
    - the state derived from previous communications
  - Information manipulation
    - the evaluation of flexible expressions based on all the above factors

Application proxy

- Maintains complete connection state and sequencing through 2 connections
  - Client to proxy
  - Proxy to server
- Doesn’t allow client to directly connect to the server
- Examples
  - Gauntlet
  - Raptor

Firewall appliance

- Integrated hardware solution
- All software including the OS comes preloaded on the platform
- Network ‘black box’ approach to the security

Stealth firewall

- ‘Invisible’
- Transparent bridge
- Doesn’t need IP address
- Interfaces are in promiscuous mode
- Accessible only from the console

What a firewall cannot protect?

- Attacks from protected network
- Authorized malicious access
- Attacks and exploits on ports that are open thru the firewall
- Attacks that do not pass through the firewall.

How firewalls works?

- Packets that pass rules are allowed
- Packets that don’t match are rejected
- Critical attack information lies in rejected packets

Logging

- Minimal logging for common traffic
- No logging for noisy traffic
- Maximum logging for the rest

OISSG

Bypassing Firewalls

OISSG

Firewalking

- Traceroute through an open port
  - Use varying TTLs
- Firewall might allow packets to port 80
- Map the n/w behind the firewall

Firewalking

- Helps determine open ports on a firewall (packet filter)
- Port scan (TCP & UDP) done with packets whose TTL is set one greater than the hop count of the filtering device.
  - If TTL error message comes back port opened
  - If nothing comes back, port is filtered

Firewalk – Prevention

• Disallow ICMP TTL exceeded messages from leaving your internal network device

Covert Channels

- A subliminal channel of communication, which hides that a message is being passed
- Not Encryption…it's concealment

Hiding in plain sight

- Embedding a message within a regular communication channel
    - E.g.. Embed data in the payload of a ‘ping’ (ICMP) packet
- Only the sender and receiver understand the hiding technique

OISSG More Sophisticated Methods

- Utilize TCP/IP header fields.
- 6 bits reserved in TCP header for future use.
- Usually not examined by security mechanisms.

Loki

• Originally presented in August 1996 in the underground magazine Phrack.

• The first generally available implementation of a covert shell.

• Loki = ‘Low Key’.

Loki: an embedded ICMP channel

• The data field in ICMP Echo Reply and type Echo Request packets are used to tunnel messages.

• The data field is meant for integrity check/ timing: rarely used/checked.

• A bi-directional Unix shell client.

007Shell: The next generation

- An improvement over previous work.
- The same program serves as either client or server.
- The distribution is split into a reusable tunneling library and a shell front end
- Employs only ping reply packets
  - Usually Ping replies are never logged!
- Root permission is required for ICMP raw socket access

AckCmd

- Written by Arne Vidstrom
- A remote command shell on Windows 2000
- Uses TCP packets for transport
- Designed to exploit a weakness in many firewall and IDS rules

OISSG AckCmd uses only TCP ACK

- Data segment of each originating ACK contains buffered command line data.

- Elicits a TCP RESET from the remote side .

- Response is then presented in a new ACK back to the originator.

- Client side TCP port 80 increases the likelihood of successful firewall traversal.

But, thankfully...

- AckCmd is plainly visible on the task list.
- The packets are not properly formatted for HTTP.
- The command line transaction is in clear text, Thus detection is possible.

?