

Testing Perimeter Security

CERT-In
Department of Information Technology
Ministry of Communications & Information
Technology
Electronics Niketan, 6 C.G.O. Complex
New Delhi- 110 003

Methodology

INSTITUTE FOR SECURITY AND OPEN
METHODOLOGIES (WWW.ISECOM.ORG)

- **Open-Source Security Testing
Methodology Manual**

- Testing components individually
- Testing the system together
 - Testing against know vulnerabilities of systems
 - Testing Packet Filtering capabilities
 - Testing Application level filtering
 - Test IDS systems

Testing Tools

- Vulnerability Scanners
 - Nessus
 - Retina etc
- Packet generation and port scanning tools
 - Lcrzoex
 - Firewalk
 - Egressor
 - hping2
 - Firewall Tester
 - nemesis
 - Nmap

Testing Routers

- Test router security
 - Benchmark the Router Configuration
 - RAT (www.cisecurity.com)
- Test the Packet filtering rule base
 - Egressor

```
C:\Rat.exe router_config_file.txt
```

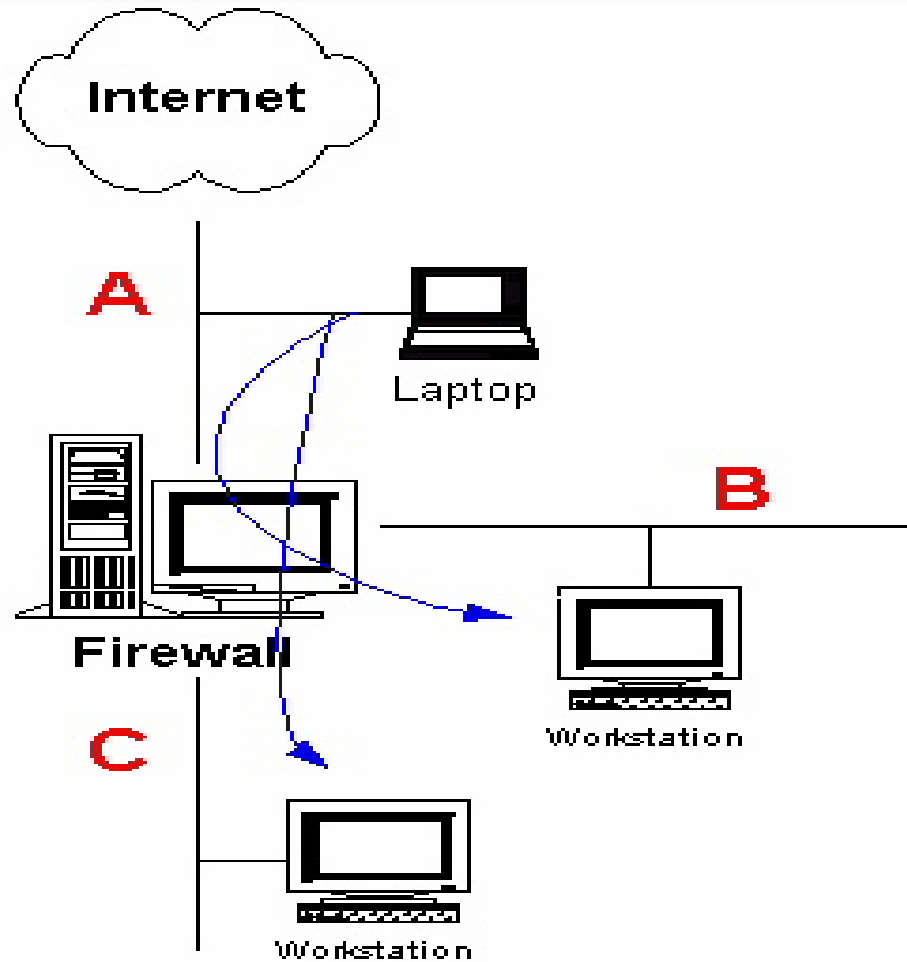
Check Firewall Rule base

Objective: Validate that the firewall is accepting ONLY the traffic that you allow

Methodology

- scanning every network segment from every other network segment to see what packets can and cannot get through the firewall

Firewall test setup



lcrzoex

How to send an TCP packet at IP level ?

```
# lcrzoex 48
```

```
source address [255.255.255.255]: 0.0.0.0
```

```
destination address [1.2.3.4]: 192.168.11.3
```

```
IP options []:
```

```
source port (between 0 and 65535)[2345]: 1234 destination port  
(between 0 and 65535)[53]: 80
```

```
bit syn (between 0 and 1)[0]: 1
```

```
bit ack (between 0 and 1)[0]:
```

```
bit rst (between 0 and 1)[0]:
```

```
seqnum (between 0 and 4294967295)[3145138187]:
```

```
acknum (between 0 and 4294967295)[2039479918]: 0 TCP options  
[]: packet's data ['hello' 0D 0A]:
```

lcrzoex

How to send an ICMP packet at IP level ?

```
# lcrzoex 65
```

```
source address [255.255.255.255]: 192.168.10.1
```

```
destination address [1.2.3.4]: 192.168.11.3 IP options []:
```

```
type (between 0 and 255)[8]: 8
```

```
code (between 0 and 255)[8]: 0
```

```
packet's data ['hello' 0D 0A]: 12345678 'my data'
```

How to send an ICMP packet at Ethernet level ?

```
# lcrzoex 68
```

```
send on which device [eth0]:
```

```
source address [aa:bb:cc:dd:ee:ff]: 00:40:33:E0:2C:42
```

```
destination address [ff:ff:ff:ff:ff:ff]: 00:40:95:46:41:BC
```

```
source address [255.255.255.255]: 192.168.10.1
```

```
destination address [1.2.3.4]: 192.168.11.3
```

```
IP options []: type (between 0 and 255)[8]: 8
```

```
code (between 0 and 255)[8]: 0
```

```
packet's data ['hello' 0D 0A]: 12345678 'my data'
```

lcrzoex

How to send an UDP packet at IP level ?

```
# lcrzoex 37
```

```
source address [255.255.255.255]:
```

```
192.168.10.1 destination address [1.2.3.4]:
```

```
192.168.11.3
```

```
IP options []:
```

```
source port (between 0 and 65535)[2345]:
```

```
1234 destination port (between 0 and  
65535)[53]:
```

```
packet's data ['hello' 0D 0A]:
```

hping2

```
#hping2 -S -p 53 -f 192.168.9.1
```

Firewalk

- Scanning the firewall system for open ports
- Mapping the rule base of the firewall
 - Firewalk -n -P135-140 -pTCP -v 172.18.10.1

Tools

- Nmap

- Scan for TCP Filtering

- ```
#nmap -v -g53 -sS -sR -P0 -O -p1-65000 -o nmap.out victim6
```

# Packet Sniffers

- Ethereal
- TCP Dump
- Snoop

# Testing IDS

- Application Level Filtering
  - HTTP Virus Wall
  - SMTP Gateway Antivirus

# Logging

- Did the firewall detect all of your scans?
- Did it set off the expected alerts?
- What traffic did it log, and how?