Securiting Samba

Introduction

Sometimes is important to configure a firewall in the system and define the interface(s) that will listening Samba4.

Securiting Samba4 AD DC with iptables

Before you configure IPTABLES, you moust to know Samba4 ports usages.

IPTABLES example using INPUT DROP Policy, and FORWARD and OUTPUT ACCEPT Policy:

```
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 53 -m state --state
NEW -j ACCEPT    # DNS
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 53 -m state --state
NEW -j ACCEPT    # DNS (UDP)
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 88 -m state --state
NEW -j ACCEPT    # Kerberos
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 88 -m state --state
NEW -j ACCEPT    # Kerberos (UDP)
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 123 -m state --state
NEW -j ACCEPT   # NTP
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 135 -m state --state
NEW -j ACCEPT   # RPC
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 137 -m state --state
NEW -j ACCEPT   # NetBIOS Name Service
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 138 -m state --state
NEW -j ACCEPT   # NetBIOS Datagram Service
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 139 -m state --state
NEW -j ACCEPT   # NetBIOS Session Service
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 464 -m state --state
NEW -j ACCEPT   # Kerberos Password
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 464 -m state --state
NEW -j ACCEPT   # Kerberos Password (UDP)
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 389 -m state --state
NEW -j ACCEPT   # LDAP
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 389 -m state --state
NEW -j ACCEPT   # LDAP (UDP)
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 445 -m state --state
NEW -j ACCEPT   # MS Directory Service
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 636 -m state --state
```

```
NEW -j ACCEPT   # LDAPS
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 1024:5000 -m state --state NEW -j ACCEPT  # DCOM
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 3268 -m state --state NEW -j ACCEPT  # MS Global Catalog
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p tcp --dport 3269 -m state --state NEW -j ACCEPT  # MS Global Cataloge SSL
 iptables -A INPUT -s 10.12.0.0/16 -i eth1 -p udp --dport 5353 -m state --state NEW -j ACCEPT  # Multicast DNS
```

Listen interfaces for Samba4

Sometimes you don't want Samba to listen on all interfaces of your host. If you limit Samba to listen only on the internal NIC(s), you don't need a firewall to prevent access from the outside.

Add the following to the [global] section of your smb.conf to bind Samba to eth0 and loopback:

```
 bind interfaces only = yes
 interfaces = lo eth1
```

The “interfaces” parameter allows various ways to restrict. See the manpage for more details. After the changes, restart Samba.