Lab 9 Notes

TA: 江易達 ccpz@ytchiang.net
Linux NAT Gateway

• Taking care of interface name / IP of external/internal interface
• Enable NAT (eth0: external, eth1: internal):
  – echo 1 > /proc/sys/net/ipv4/ip_forward
  – /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
Phase One (1/3)

- Lan: 192.168.0.0/16 on eth1
- Lan XP: 192.168.2.1
  1. Iptables –A FORWARD –d 140.113.88.160 –o eth0 –j DROP
  2. Iptables –A FORWARD –s 140.113.88.160 –i eth0 –j DROP
  3. Iptables –A FORWARD –s 192.168.10.0/24 –i eth1 –j DROP

- IP of Lan XP is changeable, hence command 3 needs to change accordingly (don’t include the IP of Lan XP)
- Ping speed.cis.nctu.edu.tw, log at record 1
- Change the IP of XP to the subnet in command #3, ping a server on the internet
Phase One (2/3)

• Blocking AVI by proxy:
  – AVI is rare now, so blocking exe
    • acl EXEFile urlpath_regex /*.exe
    • http_access deny EXEFile
  – This regular expression has false positive, you can discuss false positive/false negative on your report
Phase One (3/3)

• Transparent proxy
  – In squid.conf:
    • `http_port 3128 transparent`
  – `iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.1.1:3128`
Phase Two

• Using the following rules:
  – `iptables -A INPUT -p ICMP -icmp-type ping -i eth0 -j REJECT`
  – `iptables -A FORWARD -p TCP -dport 21 -o eth0 -j REJECT`
  – `iptables -A FORWARD -p TCP -dport 23 -o eth0 -j REJECT`

• Do the following tests, then record it:
  – In XP1
    • ping speed.cis.nctu.edu.tw
    • ftp linux.cs.nctu.edu.tw
    • telnet bs2.to
  – In XP2
    • ping (IP of linux gateway eth0)
Phase Three (1/2)

• Taking care of interface IP
• [link](http://www.smallnetbuilder.com/security/security-howto/30353-how-to-set-up-a-site-to-site-vpn-with-opENVpn)

• `./build-ca`
• `./build-key-server server`
• `./build-key remote`
• `openssl dhparam -out dh2048.pem 2048`
Phase Three (2/2)

• Copy ca.crt, remote.crt, remote.key to the other server
• Setup config file
  – local 10.1.1.2 (the external IP of server)
• openvpn /etc/openvpn/server.conf
• openvpn /etc/openvpn/client.conf