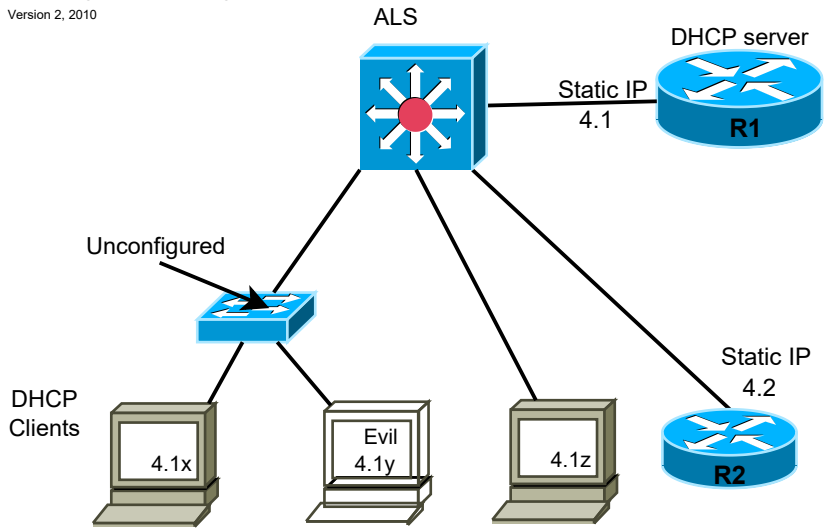
Challange3: Snooping+82+DAI

Version 2, 2010



REQUIREMENTS
0a. Configure according to the diagram shown above using /24 net's.
0b. Use passwords, enable secret, banner, SSH and no telnet everywhere
0c. Use VLAN 99 as native and management VLAN,
configure VLAN 4 everywhere else.

Step I
1a. Don't use IP-helper or DHCP relay.
1b. Configure DHCP-snooping on ALS
1c. What is option 82 (DHCP)?
1d. Enable port security and port security sticky
1e. What show command shows a) secured ports, b) port security violation mode ?
1c. CHECK: Make sure client 4.1x and 4.1y can release and renew their addresses
*** DHCP ATTACK ***
1a. Shutdown DHCP on R1 and try to make R2 a DHCP-server for 4.1x without
changing the DHCP-snooping configuration.
1b. Restore original working configuration on R1 and R2 (step 1c)

Step II
2a. configure dynamic ARP inspection (DAI) on ALS, including one trusted port
2b. What show command verifies the the DAI configuration
*** ARP ATTACK ***
2c. Ping all PCs from all PCs
2d. quickly make a note of 'arp -a' on all PCs; especially the other two PCs
2e. Shut down 4.1x and give its IP-number to Evil-PC statically
2f. Wait until the arp-cache is empty and try to ping the address 4.1x; this should not work
2g. Restore the oroginal configuration from step 2b.

Step III
3a. Enable IP source guard
3b. What command shows IP-S-G for all the interfaces on ALS ?
*** IP Source Guard ATTACK ***
3c. Make the same attack as in step II
3d. Restore

Step IV
4a. create and apply a VACL that will stop all traffic between 4.1 and 4.2
4d. create and apply a VACL that will stop all traffic to and from 4.1z MAC-address

References:

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807c4101.shtml

```
Random examples of conf' that might have something to do with anything

DLS1#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/22     ip           active       192.168.3.3                         4
DLS1#
DLS1#
DLS1#
DLS1#
DLS1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:13:72:7A:A5:1E   192.168.3.3      86068       dhcp-snooping  4     FastEthernet0/22
Total number of bindings: 1

DLS1#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/22     ip           active       192.168.3.3                         4
DLS1#
DLS1#show running
Building configuration...

Current configuration : 1857 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DLS1
!
enable secret 5 $1$t/y0$aTrRRA1njOPk/UZ9qmaI60
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
ip dhcp snooping vlan 4
ip dhcp snooping
ip arp inspection vlan 4
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
```

```
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
!    ...
!
interface FastEthernet0/21
!
interface FastEthernet0/22
 switchport access vlan 4
 switchport mode access
 ip verify source
 ip dhcp snooping limit rate 100
!
interface FastEthernet0/23
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 192.168.4.5 255.255.255.0
! no no no ip helper-address 192.168.3.1
! no no no ip dhcp relay information trusted
!
ip default-gateway 192.168.4.1
ip classless
ip http server
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 no login
line vty 5 15
 password cisco
 logging synchronous
 no login
!
end

DLS1#
```