CS646 – Spring 2018

Project #2

This project will help you bring together everything you have learned about layer 2 and layer 3 security. The objective is to create a high-level design of the security functionality deployed across this fictional national network. In this project, you will consider yourself the design engineer of a security consulting firm. Your job is to specify what is to be implemented and where it should be implemented. Specific configuration for the various models of equipment is left to a different team, however you may include configuration snippets to help illustrate your design (e.g. a sample access list), but it is not required for the project.

Deliverables:

1) A report saved as a:

Your report should:

Document your design

Explain why you chose to secure each part of the network a particular way

Explain why your design meets the requirements

Requirements:

Task 1 – "The Basics" (25 points):

a) Create a VLAN for PCs and assign all associated ports to this VLAN.
b) Create a VLAN for Phones and assign all associated ports to this VLAN.
c) Create a VLAN for Printers and assign all associated ports to this VLAN.
d) Indicate which ports are access ports and which are trunk ports.
e) Specify the router interfaces needed for each VLAN along with any other layer 3 interfaces.
f) Use sub-interfaces in your design when trunks are configured.
g) Specify how forwarding of DHCP requests to the central DHCP server (recall that this is a layer-3 technology) will be handled.

Task 2 – Basic Layer-2 Security (25 points):

a) Your design should take into consideration the number of MAC addresses that can be learned on all connected ports (consider ports connected to PCs, printers, phones, etc.).
b) Where should DHCP Snooping be deployed?
c) Where should Dynamic ARP Inspection be deployed? Remember, DAI is configured per-port.
d) How will you protect all applicable ports from Yersinia DTP attacks?
e) How will you protect all applicable ports from Yersinia STP attacks?
f) How will you handle VTP?
g) How will you handle layer 2 discovery technologies such as CDP and LLDP?

Task 3 – Layer 3 Routing (25 points):

a) Design a subnetting scheme and detail the associated routing table.

Task 4 – Basic Layer-3 Security (25 points):

a) The Update Server needs to be able to remotely power-on devices using wake-on-lan (WoL). Design your directed broadcasting security around this requirement. Research the WoL "magic packet" and design accordingly.
b) Protect against IP spoofing on all applicable switch ports.
c) Design an access list for the appropriate layer-3 ports to prevent spoofing (pay close attention to how you apply this access list, it may not be obvious to you what is ingress and what is egress). Ensure you don't break DHCP.
d) **Extra Credit:** On the same layer-3 interfaces above, protect against incoming/outgoing packets with invalid addresses.