بسمه تعالی

آزمایشگاه شبکه

دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

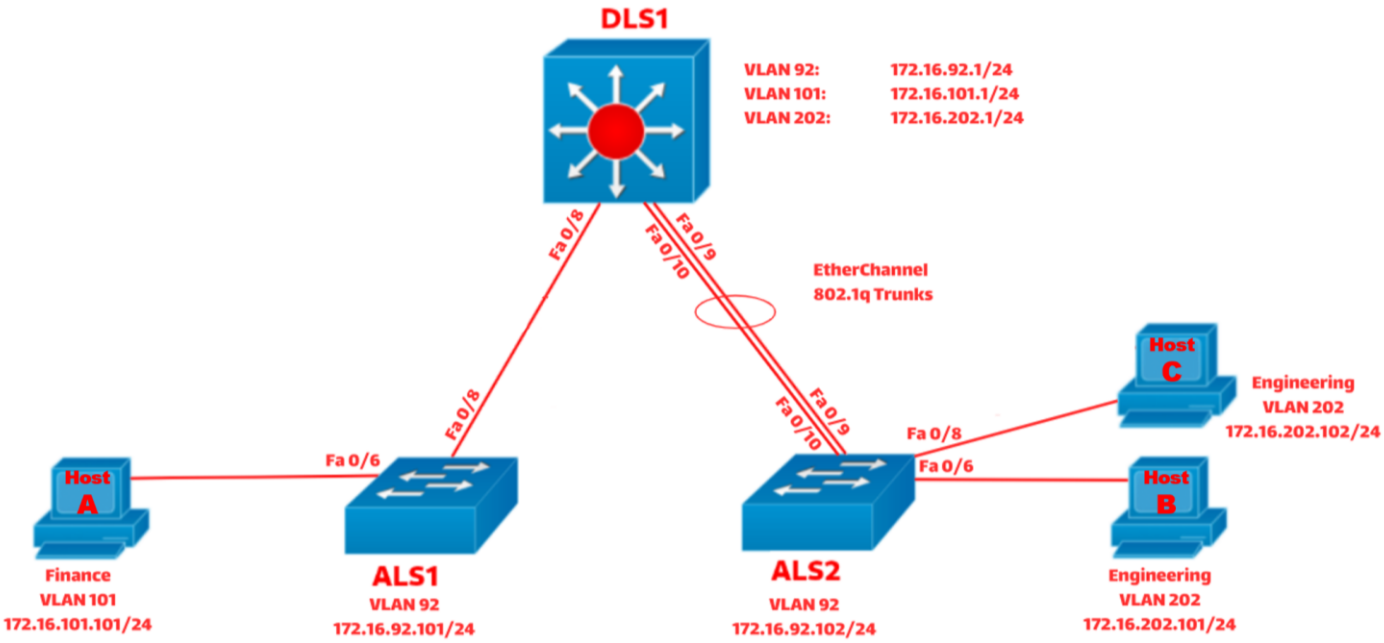
بهار ۱۴۰۲

دکتر حیدرپور، دکتر فانیان

آشنایی و محافظت در برابر حملات جعل در سوئیچ

هدف آزمایش:

در این آزمایش قرار است با مفاهیم امنیتی آشنا شویم؛ سپس به جلوگیری از ایرادات و حملات وارده در سوئیچ بپردازیم و تنظیمات را به گونه‌ای لحاظ کنیم تا از دسته‌ای از حملات جلوگیری کند.



تصویر توپولوژی آزمایش هفتم

گام اول:

اتصالات میان کامپیوترها و سوئیچ‌ها را با استفاده از کابل مناسب مطابق شکل ایجاد کنید.

گام دوم:

برای هر سوئیچ، کانفیگ NVRAM آن را پاک نموده؛ سپس اگر در مسیر flash:/ فایل vlan.dat وجود داشت با استفاده از دستور مناسب آن را پاک کنید و سوئیچ را Reload فرمایید. (دقت شود در این مرحله یک سری سوال من باب کانفیگ اولیه‌ی به‌طور خودکار از شما پرسیده می‌شود که باید برای تمامی این سوال‌ها، گزینه‌ی no را وارد نمایید)

گام سوم:

نام میزبان (Hostname) را بر روی تمامی تجهیزات اعمال کنید. همچنین تمامی پورت‌ها را به حالت خاموش (shutdown) ببرید. سپس حالت vtp transparent را بر روی سوئیچ‌ها تنظیم نمایید. پس از موارد گفته شده DNS lookup را بر روی سوئیچ‌ها غیرفعال نمایید.

گام چهارم:

بر روی سوئیچ‌ها VLAN های زیر را ایجاد نمایید.

- VLAN 101 (Finance)
- VLAN 92 (Management)
- VLAN 202 (Engineering)
- VLAN 49 (Native)
- VLAN 196 (BlackHole)

گام پنجم:

پیکربندی اترچنل را بین سوئیچ‌ها مطابق شکل ایجاد نمایید (Cisco PAgP را بین سوئیچ‌ها پیکربندی کنید). سپس با استفاده از دستور مناسب صحت درستی کار را نمایش دهید. همچنین پورت‌های trunk و access را مطابق شکل تنظیم نمایید و آنها را فعال سازید (از حالت shutdown در بیاورید). (برای trunk باید استاندارد 802.1Q رعایت شود). نهایتا تنها به VLAN های 92 ،101 و 202 اجازه دهید. دقت فرمایید حتما برای اینترفیس‌های کانفیگ شده Description قرار دهید.

گام ششم:

مابقی پورت‌ها را از VLAN 1 به VLAN 196 انتقال دهید و از غیرفعال بودن حالت trunk آنها اطمینان حاصل فرمایید.

گام هفتم:

IP آدرس‌ها را مطابق شکل به سوئیچ‌ها انتساب نمایید. همچنین ip کامپیوترها را مطابق شکل تنظیم فرمایید. نهایتا میان VLANهای 101 و 202، Inter-VLAN Routing را تنظیم نمایید. از هاست A، هاست B و هاست C را Ping کنید.

گام هشتم:

DLS1 را به عنوان سرور DHCP برای کامپیوترها تنظیم نمایید. همچنین توجه کنید که برای هر یک از vlanها یک سرویس DHCP اجرا کنید. آدرس هر کامپیوتر را از DHCP Server دریافت کنید.

گام نهم:

- بر روی یک سوییچ که امکان آن وجود دارد، تنظیمات مربوط به SSH را فعال نمایید.
- از هاست A به سوییچ مربوطه یک ارتباط توسط SSH ایجاد نمایید.
- یک ACL بر روی خطوط VTY سوییچ مربوطه به نحوی تنظیم نمایید که فقط از VLAN 202 امکان SSH وجود داشته باشد.
- مجدد از هاست‌های موجود در VLANهای مختلف به سوییچ مربوطه یک ارتباط توسط SSH ایجاد نمایید و در صورت عدم برقرای ارتباط، علت آن را توجیه کنید.

گام دهم: (لینوکس)

- دو سیستم را ریست نمایید و با لینوکس وارد شوید. (پیشنهاد می‌شود که سیستم DLS را روشن نگه دارید و سیستم‌های متصل به ALS را ریست کنید. به فرض سیستم A, B را ریست میکنیم.)
- حال با استفاده از دستور ip flush، برای دو سیستم لینوکس، ip آن را برداشته و دوباره با استفاده از دستور مناسب از DHCP، ip دریافت کنید. Ip دریافت شده را نمایش دهید. (این کار فقط جهت این می‌باشد که زمان دریافت ip از DHCP را متوجه شوید.)
- حال دوباره ip دریافت شده بر روی دو سیستم لینوکس را flush کنید.
- بر روی DLS1 با استفاده دستور "show ip dhcp binding" تمام ipهایی که تا این لحظه assign شده‌اند را مشاهده نمایید.
- با یکی از سیستم‌های لینوکس حمله‌ای صورت دهید تا DHCP Server از دسترس خارج شود. در همین حال با سیستم لینوکس دیگر در حالی که حمله برقرار می‌باشد سعی کنید از DHCP سرور دوباره ip دریافت کنید همچین بر روی DLS1 دوباره دستور "show ip dhcp binding" را نمایش دهید، در صورتی که نمی‌توانید ip دریافت کنید، علت آن را توجیه نمایید.
- حمله را متوقف نمایید و منتظر بمانید تا سیستم دیگر ip دریافت کند و DLS1 تمام ipهایی که اختصاص داده است را نمایش دهد.

گام یازدهم:

عملیات ip spoofing را انجام دهید (بر روی سیستم لینوکس). برای این کار لازم است 4 بسته با ابزار hping3 از آدرس ماشین مبدا دیگری به آدرس مقصد دیگری ارسال نمایید. (به فرض بر روی ماشین B این دستور را وارد کنید به نحوی که آدرس مبدا ماشین A و آدرس مقصد ماشین C باشد.) سعی کنید این کار را به گونه‌ای انجام دهید که ماشین دریافت کننده‌ی بسته‌ها به آنها پاسخ دهد. نهایتا روی ماشین‌های مبدا و مقصد ip با استفاده از ابزار wireshark یا tcpdump صحت این سناریو را بررسی و نمایش دهید.

زیبا باشید (: