بسمه تعالی

آزمایشگاه شبکه

دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

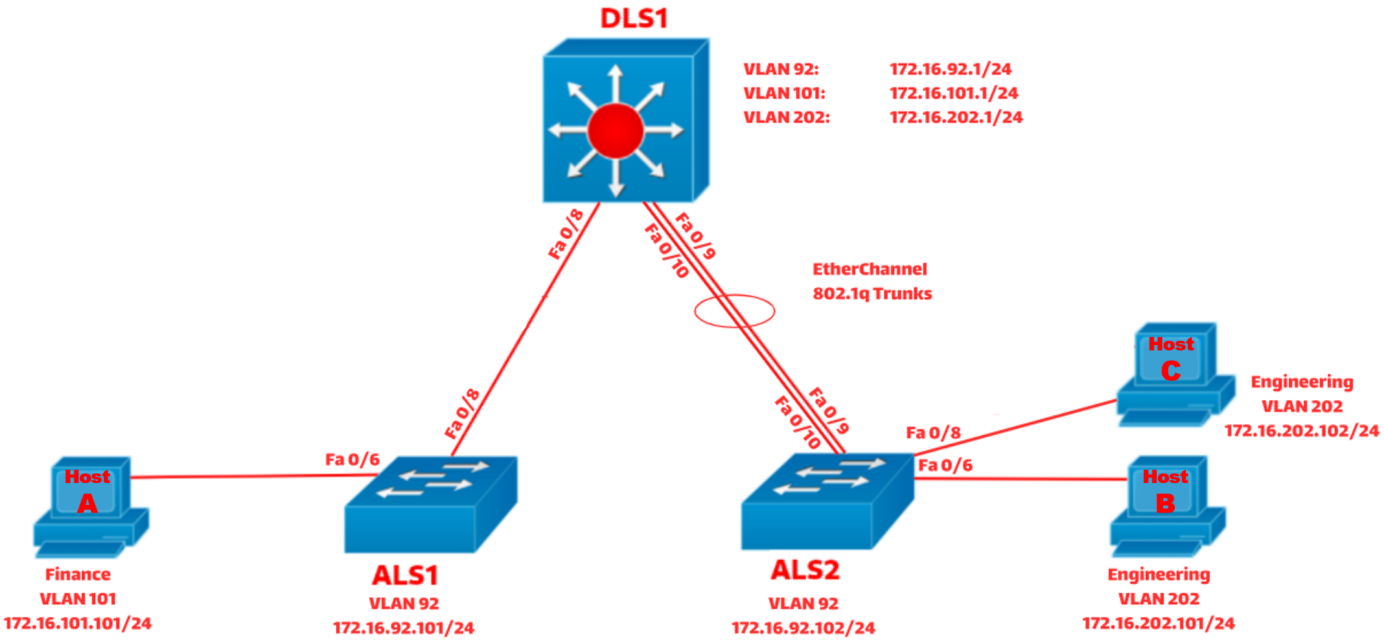
بهار ۱۴۰۲

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 ریلود 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 101، 92 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 منتسب نمایید. همچنین کامپیوترها را مطابق شکل تنظیم فرمایید. نهایتا میان VLAN های 101 و 202 اینتر ویلن روتینگ 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 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 200 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)

- بر روی یکی از کامپیوترها بررسی کنید که هیچ IP ای به اینترفیس متصل به سوئیچ اختصاص داده نشده باشد (اگر IP دارد با استفاده از دستور مناسب اینترفیس مربوطه را flush نمایید).
- سپس حمله‌ای صورت دهید تا DHCP server از دسترس خارج شود؛ در این هنگام با دستور dhclient برای اینترفیس نام برده سعی بر گرفتن IP از DHCP نمایید.
- توسط دستور "show ip dhcp binding" در سرور DHCP یا همان DLS1 تمام ipهای اختصاص یافته شده را مشاهده نمایید.

گام یازدهم (امتیازی):

عملیات ip spoofing را انجام دهید. برای این کار لازم است 4 بسته با ابزار hping3 به مقصدی با آدرس مبدا جز آدرس ماشین خود ارسال نمایید. سعی کنید این کار را به گونه‌ای انجام دهید که ماشین دریافت کننده‌ی بسته‌ها به آنها پاسخ دهد. نهایتا روی ماشین مقصد با استفاده از ابزار wireshark یا tcpdump صحت این سناریو را بررسی و نمایش دهید.

زیبا باشید :)