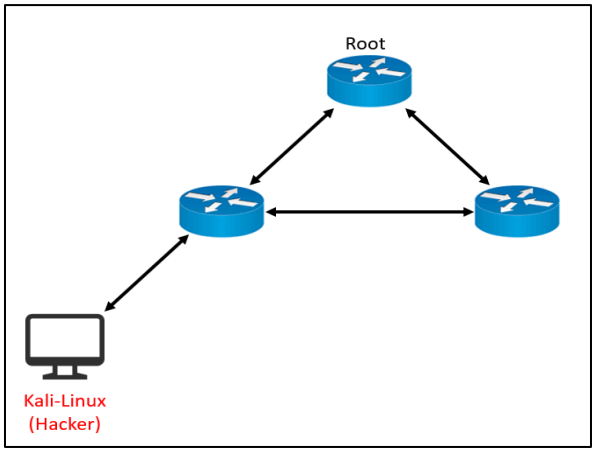
به نام خدا

پروژهٔ بخش نخست درس امنیت سایبری

دانشجویان گرامی یکی از سناریوهای زیر را انتخاب کنید و به عنوان پروژهٔ درس تحویل دهید. می‌توانید پروژه را در قالب تیم‌های تک- یا دونفره تحویل دهید. در صورت تحویل تیمی، لطفا دو عضو گروه تیم خود را به آقای حسین رضائی اطلاع دهید. در غیر این صورت فرض بر تحویل تکی پروژه خواهد بود. مهلت تحویل نهایی تا آخر خرداد ماه است. پیشنهاد می‌شود که کار را هر چه سریعتر شروع کنید و هفته به هفته با آقای رضائی هماهنگ کنید و گزارش یا سؤالات خود را با ایشان مطرح کنید. تحویل پروژه در قالب گزارش فنی و تحویل حضوری خواهد بود. کپی‌برداری از کار دیگران منجر به از دست رفتن امتیاز و کسر نمره خواهد شد. پروژه در نهایت یک چهارم از نمرهٔ بخش نخست خواهد بود. به عنوان مثال، از ۲۰ نمره بخش نخست پنج نمره به پروژه اختصاص خواهد یافت. سناریوی شمارهٔ یک هفت نمره (دو نمره اضافه) و سناریوی شمارهٔ دو پنج نمره خواهد بود.

۱- در یک پروژه شبیه‌سازی شبکه با استفاده از برنامه‌های GNS3، و VMware workstation یک مدل توپولوژی ساده به صورت مثلث ایجاد کنید یک نود kali-Linux به عنوان نود هکر در این توپولوژی در نظر بگیرید و با استفاده از برنامه Yersinia به شبکه ایجاد شده اختلال وارد کرده و نتایج را گزارش کنید.




- می‌توانید به دلخواه از router یا switch لایه ۳ استفاده کنید.
- در توضیحات خود باید ساختار این شبکه را شرح دهید و نحوهٔ ارتباط نودها با همدیگر و شناسایی نود root را بیان کنید.
- در رابطه با پیغام‌های tcn که برای اطلاع از توپولوژی شبکه بین نودها ارسال می‌شود؛ با استفاده از برنامه Wireshark این پیغام‌ها را نمایش دهید و چند مورد از آن‌ها را توضیح دهید.
- یک نود Kali-Linux به عنوان هکر به یکی از نودهای شبکه متصل کنید و با استفاده از برنامه Yersinia به شبکه مذکور حملهٔ spanning-tree انجام دهید.

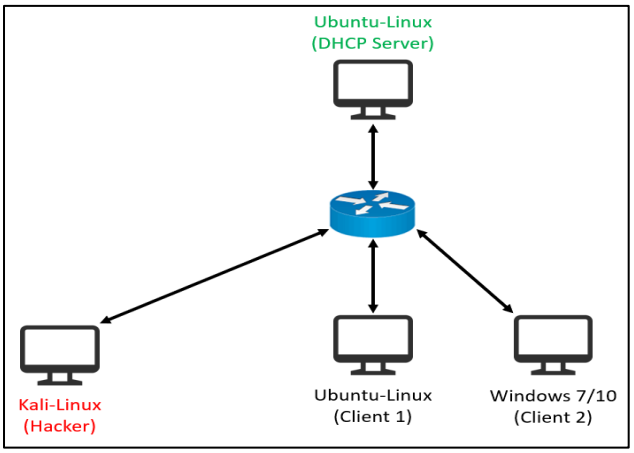
۱- به صورت مختصر در رابطه با spanning-tree و حملات مرتبط با آن را توضیح دهید.

۲- نتیجهٔ اعمال حملهٔ مذکور را با استفاده از برنامه Wireshark نمایش دهید و چند مورد از آن را تحلیل کنید (بررسی روی نود root و سایر نودها به تفکیک انجام شود).

۳- یکی از راه‌حل‌های ابتدایی جلوگیری از این حمله استفاده از دستور BPDU Guard است؛ پس از پیاده‌سازی آن مختصر توضیح دهید و نتیجه اعمال آن را با استفاده از Wireshark گزارش کنید.

---

۲- در یک پروژه شبیه‌سازی شبکه با استفاده از برنامه‌های GNS3، و VMware workstation یک DHCP Server روی Ubuntu-Linux راه‌اندازی کنید. سپس چند نود به آن متصل کرده و با استفاده از برنامه Yersinia به شبکه ایجاد شده اختلال وارد کرده و نتایج را گزارش کنید.




- می‌توانید به دلخواه از router یا switch لایه ۳ استفاده کنید.
- در توضیحات خود باید ساختار این شبکه را شرح دهید و نحوهٔ عملکرد DHCP Server و درخواست IP توسط client ها را بیان کنید.
- در رابطه با پیغام‌های DHCP برای دریافت IP که توسط client به server (وبالعکس) ارسال می‌شود؛ با استفاده از برنامه Wireshark این پیغام‌ها را نمایش دهید و چند مورد از آن‌ها را توضیح دهید.
- یک نود Kali-Linux به عنوان هکر به یکی از نودهای اصلی شبکه متصل کنید و با استفاده از برنامه Yersinia به شبکه مذکور حملهٔ DHCP انجام دهید.

۱- به صورت مختصر در رابطه با DHCP Server و حملات مرتبط با آن را توضیح دهید.

۲- نتیجهٔ اعمال حملهٔ مذکور را با استفاده از برنامه Wireshark نمایش دهید و چند مورد از آن را تحلیل کنید (بررسی روی client و Server به تفکیک انجام شود).

۳- یکی از راه‌حل‌های ابتدایی جلوگیری از این حمله را تحقیق و گزارش کنید؛ روش جلوگیری از حملات مذکور را پیاده‌سازی کنید و نتیجه اعمال آن را با استفاده از Wireshark گزارش کنید.