دانشگاه فردوسی مشهد

آزمایشگاه امنیت شبکه

تاریخ تحویل: ۱۴۰۳/۰۳/۰۱

تست نفوذ شبکه

مقدمه

تست نفوذ شبکه یک سرویس امنیتی است، که آسیب پذیری‌های امنیتی در شبکه‌ها، سیستم‌ها، میزبان‌ها و دستگاه‌ها را با استفاده از رویکردهای مخرب برای آزمایش پاسخ‌های امنیتی شبکه شناسایی می‌کند. هدف از آزمایش نفوذ شبکه، شناسایی اکسپلویت امنیتی است، قبل از اینکه مهاجمان بتوانند آن‌ها را کشف و از آن‌ها بهره برداری کنند. به زبان ساده، تست نفوذ شبکه مانند سرویسی است، که کسب و کارها برای کشف ضعیف‌ترین نقاط خود هزینه پرداخت می‌کنند. با انجام این کار، آنها به هکرهای اخلاقی اجازه می‌دهند تا با استفاده از هر ابزاری که لازم است، سعی کنند به شبکه آنها نفوذ کنند. به طور خاص، با استفاده از روش‌هایی که یک هکر واقعی استفاده می‌کند. به غیر از میزان امنیت سایبری، که باید قبل از تست نفوذ شبکه انجام شود، تست نفوذ شبکه یکی از بالاترین سطوح تضمین امنیتی یک کسب و کار را فراهم می‌کند. در سال های اخیر تست نفوذ تبدیل به رویه امنیتی اتخاذ شده توسط سازمان‌ها در سطحی گسترده شده است. درحالی که هدف اولیه تست نفوذ، آشکارسازی آسیب پذیری‌ها و یا استفاده از نقطه ضعف‌ها است. هدف اصلی یک تست نفوذ اکثر مواقع به یک هدف با یک استراتژی کلی مربوطه به کسب و کار گره خورده است.

هدف

هدف از انجام این آزمایش آشنایی با محیط شبیه‌ساز شبکه GNS3 و حملات سطح شبکه نظیر، MAC Flooding، DHCP Attack، VLAN Hopping و ARP Spoofing است. برای درک پیاده‌سازی حملات، یک توپولوژی شبکه پیش فرض در محیط GNS3 در نظر گرفته می‌شود، و حملات مورد نظر بر روی توپولوژی شبیه‌سازی می‌شوند. همچنین برای تحلیل و رفع آسیب‌پذیری مورد نظر، با نحوه جلوگیری از نفوذ و روش‌های افزایش سطح امنیت آشنا می‌شوید.

دانشگاه فردوسی مشهد

آزمایشگاه امنیت شبکه

تاریخ تحویل: ۱۴۰۳/۰۳/۰۱

فعالیت‌های درون کلاسی

۱. مسئله

- دانلود، نصب و راه‌اندازی محیط شبیه‌ساز GNS3
- طراحی توپولوژی پیش‌فرض در نظر گرفته شده، در محیط شبیه‌ساز مورد نظر
- راه‌اندازی و تنظیمات مسیریابی و میزبان‌های مورد نظر
- ارسال و دریافت چند بسته در توپولوژی ایجاد شده و گزارش‌گیری

۲. نیازمندی‌ها

- محیط شبیه‌ساز GNS3

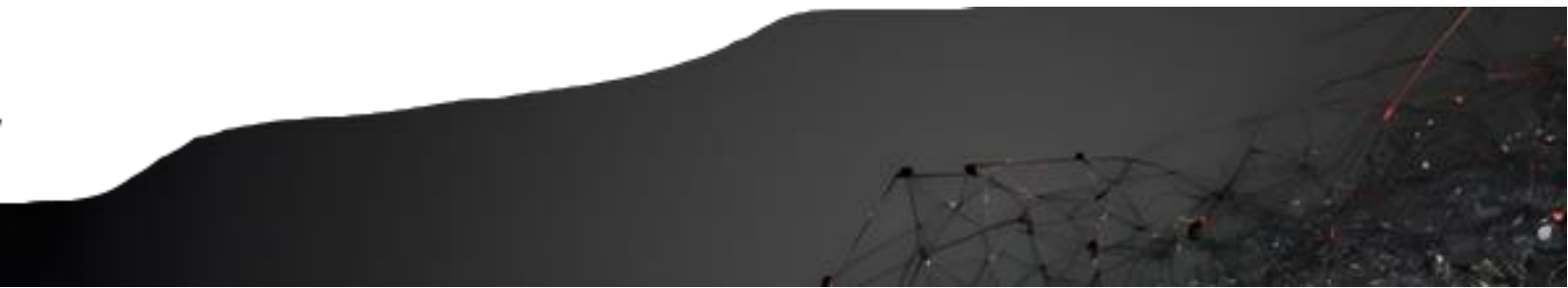
https://www.gns3.com/software/download

https://www.gns3.com/software/download-vm

- سیستم عامل کالی

https://www.kali.org/get-kali/#kali-platforms

- ابزارهای macof، yesinia و Ettercap



دانشگاه فردوسی مشهد

آزمایشگاه امنیت شبکه

تاریخ تحویل: ۱۴۰۳/۰۳/۰۱

تکالیف

۱. مسئله

الف) نظری

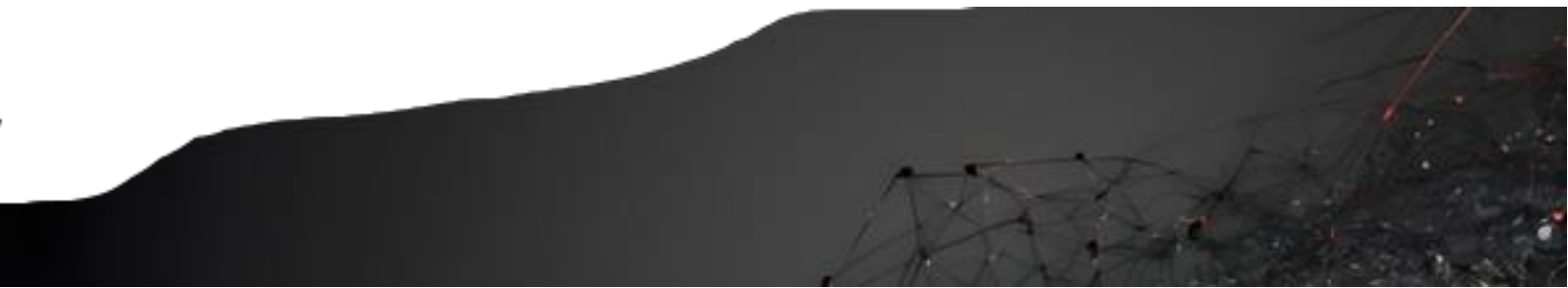
- تفاوت تست نفوذ و ارزیابی آسیب‌پذیری را بیان کنید.
- مکانیزم‌های امنیتی برای مقابله با هر یک از حملات MAC Flooding، DHCP Attack، VLAN Hopping و ARP Spoofing را شرح دهید.

ب) عملی

- توپولوژی مناسب شبکه برای اجرای هر یک از حملات MAC Flooding، DHCP Attack، VLAN Hopping و ARP Spoofing را ایجاد کرده و شبیه‌سازی حملات را انجام دهید.
- با ایجاد تنظیمات مناسب در توپولوژی آسیب پذیر و یا به‌کارگیری ابزارهای دفاعی، به‌منظور جلوگیری از هر یک حملات مورد نظر، حداقل یک رویکرد را شبیه‌سازی کنید.
- تمامی بخش‌های پیشین را مستندسازی کنید.

۲. نکات قابل توجه و معیارهای ارزیابی

- مهلت تحویل تکلیف، ساعت ۲۳:۵۹ روز شنبه مورخ ۱۴۰۳/۰۳/۰۱می‌باشد.
- دانشجویان گرامی تا تاریخ مشخص شده فرصت دارند تا فایل‌های زیر را در سامانه مجازی درس در آزمایش ۵ آپلود نمایند. در غیر اینصورت، تاخیر در ارسال پاسخ مشمول کسر نمره خواهد شد.



- فایل‌های کدهای اجرایی و پیاده‌سازی شده، ضبط صفحه همراه با توضیح تکلیف و گزارش مستند شده بایستی در قالب فشرده تحت عنوان StudentName_StudentID (به جای StudentName نام خانوادگی و به جای StudentID شماره دانشجویی خود را وارد نمایید.)
- این تکلیف به‌صورت فردی تعریف شده و قابل انجام است.

چه عواملی باعث می شود از این فعالیت نمره کسب نکنید:

- عدم تحویل فایل ها در سامانه vu
- فقط انجام بخش تئوری بدون انجام بخش عملی
- عدم ضبط ویدیو بر روی بخش عملی
- مشاهده شباهت بیش از حد معقول
- عدم تسلط به موضوع در جلسه ارائه سر کلاس

چه عواملی باعث می شود نصف نمره را کسب کنید؟

- تحویل فایل در سامانه vu، اما عدم ارائه در کلاس درس یا غیبت در روزی که ارائه باشد و نام فرد یا تیم برای ارائه تعیین شده باشد.
- عدم تحویل در زمان مقرر و تحویل با تاخیر.