آزمایشگاه امنیت شبکه

Nmap - Zmap

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با دو ابزار ساده شبکه آشنا شوند.

آزمایش ۱-۱۰:

- وب سایت دانشگاه (iut.ac.ir) و وب سایت دانشگاه ام آی تی (mit.edu) را در نظر بگیرید.
- با استفاده از ابرازهایی همچون nmap، zmap، maltego و... اقدام به نگاشت شبکه و بدست آوردن اطلاعات کنید. (اینکه از چه ابزارهایی استفاده می‌کنید انتخاب شماست اما nmap ضروری است.)
- تا حدی که می‌توانید از آن‌ها اطلاعات کسب کنید و آن‌ها را گزارش کنید.

آزمایش ۲-۱۰:

- از کدام وب سایت اطلاعات بیشتری توانستید کسب کنید؟
- فرض کنید اطلاعات A را از دانشگاه اول کسب کرده‌اید اما همان اطلاعات را از دانشگاه دوم کسب نمی‌کنید (یا برعکس). دلیل این امر چیست؟(سیاست مورد استفاده در شبکه دانشگاهی که اطلاعات A را فاش نکرده را گزارش کنید.)

آزمایش ۳-۱۰:

- فرض کنید در یک نقطه حساس شبکه یک IDS/IPS وجود دارد که از اسکن پورت‌ها جلوگیری می‌کند.
- فرض کنید یک هاست در آن قسمت از شبکه وجود دارد که از پشته دوگانه برای پشتیبانی از IPv۶ استفاده می‌کند.
- چگونه می‌توانید از TCP SYN برای اسکن پورت استفاده کنید درحالیکه IDS/IPS هیچ هشداری صادر نکنند؟

آزمایش ۴-۱۰:

- سؤال قبل از جهت برعکس و در حضور firewall و NAT در نظر بگیرید.
- فرض کنید هاست موجود در سؤال قبل (با همان شرایط) اقدام به ارسال درخواست یا اطلاعات به یک سرور بیرونی می‌کند که توسط firewall فیلتر شده است.
- به نظر شما این درخواست یا اطلاعات چگونه در حضور فیلترینگ firewall می‌تواند به مقصد در بیرون از شبکه برسد؟

***آزمایش ۵-۱۰:**

- یک برنامه بنویسید که امکان زیر را داشته باشد:
  - یک پورت مشخص روی رنج کامل آدرس‌های IP را اسکن کند بطوریکه نیاز به نگه‌داری ارتباط نباشد (stateless باشد) و همچنین نیاز به برقراری واقعی یک ارتباط نداشته باشد و مستقیماً یک بسته TCP را به اترنت ارسال کند.
- برنامه‌ای که نوشتید را از لحاظ سرعت با nmap مقایسه کنید! چه نتیجه‌ای می‌گیرید؟