به نام خدا

تکلیف کلاسی مرتبط با ابزار nmap

سلام،

امیدوارم که دو جلسه‌ی مرتبط با ابزار nmap برای شما مفید بوده باشد و آشنایی مقدماتی با این ابزار کاربردی را کسب کرده باشید. برای یادآوری برخی موضوعات مطرح شده و مقداری کنکاش بیشتر در ویژگی‌های nmap می‌خواهیم کمی بیشتر با این ابزار کار کنیم.

برای شروع لازم است که شما nmap را نصب کرده باشید و یک شبکه‌ی محلی هم در اختیار داشته باشید. بعد از راه‌اندازی کارهای زیر را انجام دهید و نتیجه را گزارش کنید. اگر بتوانید تحلیلی از آنچه رخ می‌دهد نیز در برخی از موارد ارائه دهید، نتیجه کامل‌تر خواهد بود.

- **گام اول**

در گام اول سعی کنید میزبان‌های زنده در محدوده‌ی شبکه‌ی محلی خود را پیدا کنید. برای این کار باید ابتدا محدوده‌ی آدرس IP شبکه را پیدا کنید و سپس آن محدوده را اسکن کنید.

- **گام دوم**

سعی کنید با انواع روش‌های اسکن، سیستم‌عامل تجهیزی که به آن متصل هستید و همچنین درگاه‌های باز آن را شناسایی کنید. روش‌های اسکن استفاده شده را توضیح دهید.

- **گام سوم**

با استفاده از امکاناتی که nmap در اختیار شما می‌گذارد، بخش‌های اختیاری بسته‌ی ارسالی برای اسکن را مدیریت کنید. برای مثال از ویژگی‌های Loose source routing, Strict source routing و timestamp در بسته‌های IP بهره ببرید و تصویر بسته‌های ارسالی را با استفاده از wireshark ارائه کنید.

چند سوال

در ادامه به این چند سوال نیز پاسخ دهید.

1 - عملیات تشخیص نسخه سرویس و سیستم‌عامل به چه طریق اتفاق می‌افتد؟ آیا می‌توان یک OS جدید را به پایگاه داده nmap اضافه کرد؟ چگونه؟

2 - توضیح دهید که چرا استفاده از روش UDP برای اسکن تمامی درگاه‌های یک میزبان زمان‌بر است؟

3 - تفاوت SYN Scan و Connect Scan چیست؟

4 - برای عبور از سامانه‌های تشخیص نفوذ (IDS) nmap چه راهکاری را پیشنهاد می‌دهد؟

5 - دسته‌بندی نویسه‌های اسکن در nmap کدام است؟ فایده‌ی کلی استفاده از این نویسه‌ها چیست؟

موفق باشید :)