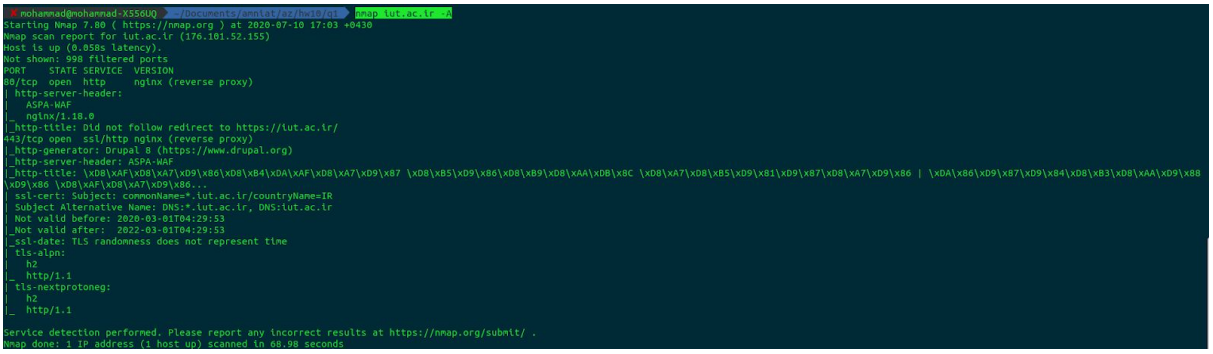
محمد عبدالهی 9530153

1. از طریق دستور $nmap\ iut.ac.ir\ -A$ سایت اول را چک کردم:



از طریق دستور $nmap\ mit.edu\ -A$ سایت دوم را چک کردم:

2. از سایت iut اطلاعات بیشتر بدست آمد.
شاید دلیل اینکه از سایت iut اطلاعات بیشتری را کسب میکنیم این باشد که دانشگاه از سیستم های اپن سورس برای پیاده سازی ساختار خود استفاده کرده اما در mit تمام این ها به شرکت های بیرونی سپرده شده.

3. سیستم هایی که ipv6 را پشتیبانی میکنند لازم است که ipv4 را هم پشتیبانی کنند در نتیجه ممکن است در نتیجه این حالت مشکلاتی برای ids/ips ایجاد شود که ممکن است بدلیل فضای گسترده ipv6 یا ساختار ماژولار ipv6 ایجاد شود همچنین در حالت کلی وقتی کانکشن ایجاد شود سیستم حمله کننده پس از دریافت بسته syn ack اگر بسته drop را ارسال کند از کانکشن خارج شده و ids ips هم لاگ نمیکند.

4. معمولا بسته های udp مربوط به dns از فایروال به راحتی عبور میکنند. میتوان از این ضعف برای دور زدن فایروال استفاده کرد. در این حالت میتوان با قرار دادن اطلاعات در dns request ارسال را به dns server فرستاد و ان هم درخواست ما را به سرور مورد نظر ارسال میکند.