هوالحق

تمرین کامپیوتری شماره ۱
مبانی امنیت شبکه، بهار ۱۴۰۳

در این تمرین به راه اندازی یک سرویس دهنده‌ی پروتکل HTTPS پرداخته و تأثیر وجود این پروتکل بر ساختار ترافیک شنود شده را بررسی خواهیم کرد. برای انجام این تمرین نیاز به یک نسخه از توزیع Ubuntu سیستم عامل لینوکس (ترجیحاً نسخه 22.04 LTS) خواهید داشت. همچنین برای راهنمایی شما در هر قسمت لینک دستورالعمل پیشنهادی تأمین شده است.

۱) راه اندازی سرور HTTP با احراز هویت کاربری

- در این قسمت شما می‌بایست یک سرور Apache به صورت محلی راه اندازی کنید. برای این کار می‌بایست وب سرور Apache را با توجه به دستور العمل‌های موجود نصب کنید. برای این کار می‌توانید از این لینک استفاده کنید.
- پس از نصب Apache، با باز کردن مرورگر و تایپ آدرس 127.0.0.1 می‌توانید صفحه پیشفرض و راهنمای پیکر بندی Apache را مشاهده کنید. هدف از این تمرین پیکربندی یک سرویس وب نیست، فلذا همین صفحه برای ایجاد یک پروسه احراز هویت کاربری کفایت خواهد کرد.
- برای ایجاد یک روند احراز هویت کاربری برای صفحه موجود در آدرس 127.0.0.1 از راهنمای تأمین شده در این لینک استفاده کنید. پس انجام این مرحله، با تایپ آدرس 127.0.0.1، مرورگر یک کادر برای ورود اطلاعات احراز هویت نمایش خواهد داد که با تأمین صحیح آن صفحه اصلی نمایش داده شده و در غیر این صورت با خطای 401 Unauthorized روبرو خواهید شد. **دقت داشته باشید که صرفاً از نام خانوادگی خود برای نام کاربری احراز هویت htpasswd استفاده کنید.** نام کاربری شما می‌بایست در تصاویر موجود در گزارش موجود باشد.
- در این مرحله اقدام به نصب ابزار Wireshark نمایید. این ابزار امکان ضبط بسته‌های رد و بدل شده روی درگاه‌های کامپیوتر را به شما خواهد داد.
- پس از نصب Wireshark، با استفاده از این ابزار به ضبط بسته‌های منتقل شده روی درگاه lo (loopback) از سیستم خود اقدام نمایید. تمامی ترافیک آدرس 127.0.0.1 (localhost) از طریق این درگاه منتقل می‌گردد. پس آغاز عملیات ضبط بسته‌ها، مرورگر خود را باز کرده و با تایپ آدرس 127.0.0.1 و وارد کردن اطلاعات کاربری، وارد صفحه اصلی شوید. پس از این کار، عملیات ضبط بسته توسط Wireshark را متوقف سازید. در این مرحله باید تعدادی بسته از نوع HTTP و TCP توسط ابزار Wireshark ضبط شده باشد.
- با بررسی محتوای سربرگ بسته‌های HTTP ضبط شده در محیط ابزار Wireshark، پارامتر Authorization را بیابید. محتوای این پارامتر شامل نام کاربری و رمز عبور وارد شده توسط کاربر با فرمت Radix64 می‌باشد. با استفاده از خود ابزار Wireshark و یا ابزارهای آنلاین موجود، به تبدیل این رشته به فرمت ASCII اقدام کنید.
- علت امکان شنود اطلاعات احراز هویت کاربری به صورت خام و رمز نشده را بیان کنید.

هوالحق

تمرین کامپیوتری شماره ۱
مبانی امنیت شبکه، بهار ۱۴۰۳

۲) راه اندازی سرور HTTPS با احراز هویت کاربری

- در این قسمت می‌بایست یک گواهی Self-Signed با استفاده از ابزار OpenSSL ایجاد کرده و پیکربندی پروتکل HTTPS را روی سرور راه‌اندازی شده در قسمت قبل انجام دهید. برای این کار می‌توانید از راهنمای این لینک استفاده کنید.
- پس از پیکربندی، می‌بایست امکان ورود به صفحه اصلی 127.0.0.1 را با تأمین اطلاعات احراز هویت کاربری و تحت پروتکل HTTPS داشته باشید. در صورت اعلام هشدار توسط مرورگر مبنی بر عدم اعتبار گواهی تأمین شده (به علت Self-Signed بودن)، آن را نادیده بگیرید.
- مجدداً با استفاده از ابزار Wireshark به ضبط بسته‌های رد و بدل شده در حین دسترسی و تأمین اطلاعات احراز هویت کاربری روی آدرس 127.0.01 بپردازید. آیا امکان مشاهده پارامتر Authorization و استخراج نام کاربری و رمز عبور وارد شده توسط کاربر وجود دارد؟
- علت عدم امکان شنود اطلاعات احراز هویت کاربری را بیان کنید.
- پیام‌های منتقل شده در فرآیند Handshake را توسط Wireshark رصد کرده و سپس آن‌ها را با آنچه در متن درس آشنا شده‌اید مطابقت دهید. همچنین بیان دارید که کدام یک از مراحل Handshake را مشاهده و کدام‌ها را مشاهده نکرده‌اید. آیا تمامی پیام‌های الزامی رصد شده است؟ آیا پیامی از پیام‌های اختیاری مابین کلاینت و سرور رد و بدل شده است؟ مشاهدات و تفسیر خود را گزارش نمائید.

نکات

* گزارش خود را در قالب **تنها** یک فایل PDF با نام شماره دانشجویی خود ارسال نمائید.

* در هر مرحله از انجام این تمرین، تصاویر مناسب از انجام عملیات را در گزارش الحاق کنید. **این تصاویر می‌بایست شامل ساعت و تاریخ سیستم باشند.** برای این کار می‌توانید کادر مربوط به زمان سیستم عامل را در هنگام تصویربرداری باز نموده، و یا یک Terminal که دستور «**date**» درون آن اجرا شده است را در هنگام تصویربرداری در کنار مجموعه قرار دهید.

* دستورات، مراحل و نحوه پیکربندی و پاسخ به سؤالات هر بخش می‌بایست درون گزارش ذکر گردد.

* گزارش شما باید لازم و در عین حال کافی باشد. تعداد صفحات یک گزارش کیفیت آن را تعیین نخواهد کرد.