تمرین شماره ۱

درس امنیت شبکه های کامپیوتری

در این تمرین با نرم افزاری آموزشی برای رمزنگاری، سیستم‌عامل لینوکس و حملات فعال آشنا خواهیم شد.

به نام خدا
تمرین شماره ۱
درس امنیت شبکه‌های کامپیوتری
نیمسال دوم سال تحصیلی ۹۶-۹۵
مدرس: محمدرضا رازیان
کمک‌مدرس: مصطفی عبداللهی

سلام.

توجه ۱: ابتدا تمرین هر بخش را به طور کامل بخوانید و بعد به حل آن بپردازید (برخی از نکات در انتهای بخش آمده است).

توجه ۲: در پاسخ‌های تشریحی، برای ما این مهم است که شما فهم خود را مکتوب کنید نه اینکه ترجمه کنید و یا عیناً متنی را از جایی بنویسید.

توجه ۳: گزارش حل تمرین‌ها را به زبان فارسی تایپ شده باشد.

توجه ۴: تمام سعی خود را بکنید که گزارش نویسی را **زیبا، مرتب و خوانا** انجام دهید. علت این امر این است که در محیط کاری خیلی از گزارش‌های خود را باید به صورت گفته شده تحویل دهید. دوستان! واقعاً گزارش نویسی جزئی از کار سپرده شده به ما است که مثل بقیه اجزای کار باید آن را هم به خوبی انجام دهیم. در صورتی که بهترین کار را انجام دهید اما نتوانید به بهترین وجه گزارشِ انجام آن را ارائه دهید کار انجام شده به بهترین وجه ارزیابی نخواهد شد. نکته آخر اینکه الزاماً ما باید فقط گزارش کاری را که انجام داده‌ایم ارائه دهیم نه فراتر از کار انجام شده.

توجه ۵: کپی دهنده (کپی دهندگان) و کپی گیرنده (کپی گیرندگان) نمره ۱۰۰ - خواهند گرفت (حتی در اولین بار!).

توجه ۶: گزارش حل تمرین به صورت یک پوشه زیپ شده (Zipped) با شرایط زیر ایمیل شود.

To	en.m.abdollahy@gmail.com
CC	mrazian.email@gmail.com
نام فایل:	LastName#-ns-hw-1
عنوان ایمیل:	LastName #-ns-hw-1

توجه ۷: نمره تمرین در سایت درس قرار داده خواهد شد.

توجه ۸: فرصت انجام این تمرین لغایت ۱۳۹۶/۰۲/۱۱ ساعت ۲۳:۵۹:۵۹ می باشد. به ازای هر ساعت تاخیر ۳ درصد از نمره شما کسر خواهد شد (مثلا ساعت ۰۰:۰۰:۰۰ تا ۵۹:۵۹:.. سه درصد کسر خواهد شد) (به استثنای شرایط بسیار بسیار خاص برای دانشجوی با این شرایط).

به نام خدا
تمرین شماره ۱
درس امنیت شبکه‌های کامپیوتری
نیمسال دوم سال تحصیلی ۹۶-۹۵
مدرس: محمدرضا رازیان
کمک‌مدرس: مصطفی عبداللهی

بخش اول (۲۰ نمره)

در این بخش شما با نرم‌افزار CrypTool آشنا خواهید شد (سایت نرم‌افزار: https://www.cryptool.org/en). نرم‌افزار CrypTool نرم افزاری رایگان برای شناخت بهتر الگوریتم‌های رمزنگاری است. ما با نسخه دو مربوط به سیستم عامل ویندوز این نرم‌افزار کار می‌کنیم. این نرم‌افزار را می‌توانید از اینجا دانلود نمایید.

متن اصلی: نام و نام خانوادگی شما به انگلیسی
کلید: شماره دانشجویی شما به عنوان *کلید* می‌باشد

الف) با استفاده از نرم‌افزار CrypTool عملیات رمزگذاری و رمزگشایی را برای الگوریتم DES در مود کاری OFB انجام دهید (راهنمایی: راهنمای موجود در نرم‌افزار (help)، می‌تواند آموزش دهنده خوبی برای شما باشد. مثال‌های کاملی در help موجود است یعنی نیازی نیست که خودتان الگوریتم DES را در آن ایجاد کنید و کافی است متن و کلیدتان را در مثال آماده موجود در نرم‌افزار قرار دهید و از خروجی آن عکس بگیرید).
ب) اثر بهمنی را تعریف کنید و آن را با استفاده از نرم‌افزار مورد آزمون قرار دهید.
ج) در نرم‌افزار نمونه‌ای از Cryptanalysis به شیوه تحلیل فرکانسی را بر روی رمز سزار را بیابید.متنی رمزشده که با کلید رقم آخر شماره دانشجویی شما با سزار رمز شده را به این نمونه بدهید تا آن را بشکنند. از صفحه‌ای که نشان دهنده شکسته شدن رمز می‌باشد تصویری بیاورید.
توجه: تصویر و توضیح مختصر از مراحل کار با نرم‌افزار آورده شود. تصاویر باید به گونه‌ای باشند که بعد از اینکه بزرگ نمایی (Zoom In) روی آن‌ها انجام گرفت جزئیاتش قابل مشاهده باشد.

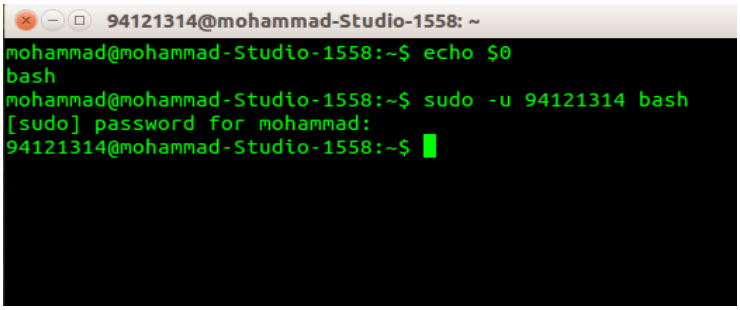
بخش دوم (۴۰ نمره)

در این بخش می‌خواهیم با برخی از دستورات کاربردی در سیستم عامل لینوکس آشنا شویم (در صورتی که سیستم عامل لینوکس بر روی رایانه خود ندارید می‌توانید آن را به طور مستقل در کنار سیستم عامل ویندوزی خود و یا به صورت مجازی –با استفاده از VMware یا VirtualBox– بر روی سیستم عامل ویندوزی خود نصب کنید. پیشنهاد می‌شود توزیع اوبونتو را نصب کنید). هدف از این تمرین آشنایی با مواردی است که در تمرین‌های بعد به کار می‌رود. همفکری و مشورت با دیگر اعضای کلاس برای انجام این بخش آزاد و بلامانع است اما پاسخ را در نهایت هر فرد با فکر خودش بنویسد.
۱) درباره هر یک از دستورات زیر تحقیق کنید و توضیح دهید چه کاربردی دارند (در حد یک خط). برای هر کدام یک مثال ساده و کوچک به همراه تصویر اجرای آن در سیستم عامل لینوکس بیاورید (خودتان دستور را اجرا کنید).

۱. useradd
۲. passwd

توجه مهم: از اینجا به بعد در تصاویری که می گیرید نام user در خط فرمان (در Prompt) باید شماره دانشجویی شما باشد مانند شکل زیر

به نام خدا
تمرین شماره ۱
درس امنیت شبکه‌های کامپیوتری
نیمسال دوم سال تحصیلی ۹۶-۹۵
مدرس: محمدرضا رازیان
کمک‌مدرس: مصطفی عبداللهی



برای این کار باید یک user با نام شماره دانشجویی خود ایجاد کنید و مانند تصویر بالا تغییر user دهید و Prompt را عوض کنید.

۳. دستور cut
۴. دستور wc
۵. دستور head
۶. دستور sort
۷. دستور uniq
۸. دستور grep
۹. دستور awk
۱۰. دستور tr
۱۱. md5sum
۱۲. sha512sum

۲) با استفاده از زبان Shell Script (در لینوکس) برنامه‌ای بنویسید که پردازش‌های زیر را روی محتویات فایل info.log (در پوشه تمرین قرار دارد) انجام دهد. کد مربوط به هر قسمت و تصویر خروجی (و نه متن فایل‌های خروجی) را در گزارش بیاورید.

۱. محتویات فایل info.log را بر اساس نام خانوادگی مرتب کنید و در فایل دیگری بریزید و محتویات فایل جدید را نمایش دهید.
۲. بیشترین و کمترین نمره درس Network و نام خانوادگی افرادی که این نمره را گرفته‌اند نمایش دهید.
۳. میانگین نمرات هر دانشجو را محاسبه کرده و یک ستون جدید با نام average به فایل اضافه کنید و محتوای فایل جدید ایجاد شده را نمایش دهید.

میانگین نمرات هر درس را محاسبه کنید و به تفکیک نام درس نمایش دهید.

به نام خدا
تمرین شماره ۱
درس امنیت شبکه‌های کامپیوتری
نیمسال دوم سال تحصیلی ۹۶-۹۵
مدرس: محمدرضا رازیان
کمک‌مدرس: مصطفی عبداللهی

بخش سوم – (انجام به صورت گروه‌های دو یا سه نفره) (۴۰ نمره)

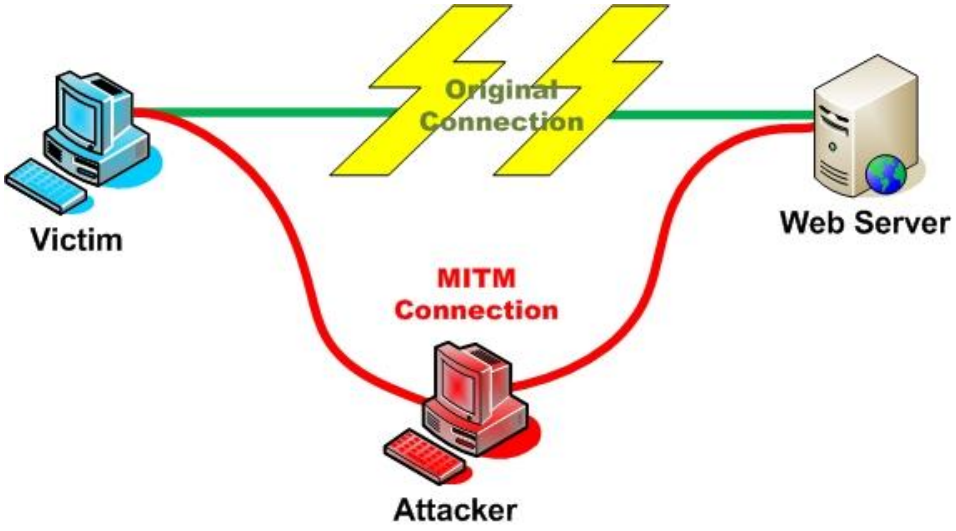
شما فقط مجازید از دانش حاصل از انجام این تمرین در مقاصد اخلاقی و مثبت استفاده کنید. به یاد داشته باشید شما یک کارشناس آی.تی. هستید و نه یک...

توجه: نام گروه و اعضای گروه را تا تاریخ ۳۱فروردین به تدریسیار مربوطه ایمیل نمایید (مثال از نام گروه: Roshd Hacker Team). هر گروه یک گزارش کافی است.

روال حمله:

در درس با حملات فعال (Active) آشنا شدید. در این بخش می‌خواهیم با حمله ARP cache poisoning (ARP spoofing) که یک حمله فعال است آشنا شویم. در این حمله، حمله کننده بسته های جعلی از پروتکل ARP را به یک شبکه محلی ارسال می‌کند و خود را به جای **Web Server** جا می زند.

برای انجام این تمرین لازم است تا شبکه ای با حداقل دو رایانه ایجاد کنید (مانند شکل زیر البته Attacker می تواند خود نیز نقش web server را ایفا کند) که این رایانه ها را با استفاده از یک مودم/روتر خانگی (که برای اینترنت ADSL استفاده می شود) می توانید شبکه کنید. برای ایجاد Web Server از نرم افزار Apache و یا Setoolkit استفاده کنید. سایت درس را در آن قرار دهید. حمله کننده، حمله را این گونه طراحی می کند که وقتی Victim می خواهد سایت درس را ببیند به آدرس Attacker وصل می شود و وب سایت درس را از Web Server حمله کننده (Attacker) می بیند. حمله کننده هم اطلاعات این سایت را عوض کرده (مثلا در بخش Important Info یک اطلاعیه جعلی قرار داده) است.



الف) روال انجام این حمله (نحوه انجام حمله برای تغییر اطلاعات سایت درس و تشکیل سایت جعلی) و ابزارهای مورد نیاز را به طور دقیق توضیح دهید (مثل یک راهنمای مرحله به مرحله). پس از انجام فعالیت فوق از سیستم **Victim** سایت جعلی را مشاهده کرده و **Screen shot** بگیرید.

از مراحل مختلف **Screen shot** گرفته و در گزارش حل تمرین بیاورید. آدرس **hostname** را به شماره دانشجویی خود تغییر دهید،

به نام خدا
تمرین شماره ۱
درس امنیت شبکه‌های کامپیوتری
نیمسال دوم سال تحصیلی ۹۶-۹۵
مدرس: محمدرضا رازیان
کمک‌مدرس: مصطفی عبداللهی

آدرس مودم خانگی خود را به گونه ای تغییر دهید که دو رقم انتهایی شماره دانشجویی تان، رقم های انتهایی آن باشد برای مثال **192.168.1.studentID**

ب) به دنبال سایتی بگردید که برای **Login** یا سایر فعالیت هایی که به صورت **Input** انجام می‌شوند از **Encryption** استفاده نشده باشد و با استفاده از روش **Arp poisoning** (**Ettercap - Wireshark**) نام کاربری و کلمه عبور **Victim** را استخراج نمایید (توضیح کامل روش انجام کار) .

ج) حمله های **Pharming** و **DNS Spoofing** و **Phishing** را توضیح دهید.

د) راه مقابله با حمله های سوال ج چیست؟

مرد فقیری بود که همسرش کره می ساخت، آن زن کره ها را به صورت دایره های یک کیلویی می ساخت. مرد آنرا به یکی از بقالی های شهر می فروخت و در مقابل مایحتاج خانه را می خرید. روزی مرد بقال به اندازه کره ها شک کرد و تصمیم گرفت آنها را وزن کند. هنگامی که آنها را وزن کرد، اندازه هر کره ۹۰۰ گرم بود. او از مرد فقیر عصبانی شد و روز بعد به مرد فقیر گفت: دیگر از تو کره نمی خرم، تو کره را به عنوان یک کیلو به من می فروختی در حالی که وزن آن ۹۰۰ گرم است. مرد فقیر ناراحت شد و سرش را پایین انداخت و گفت: ما ترازویی نداریم و یک کیلو شکر از شما خریدیم و آن یک کیلو شکر را به عنوان وزنه قرار می دادیم...

موفق باشید.