سری پروژه‌های درس امنیت

بهار ۱۴۰۲

آخرین ویرایش: ۱۵ فروردین ۱۴۰۲ در ساعت ۸ و ۵۱ دقیقه

پروژه

مقدمه

در این سری از پروژه‌ها، از دانشجویان گرامی انتظار می‌رود تا بتواند با استفاده از ابزارهای موجود، یکی از پروژهای معرفی شده را پیاده سازی کند. برای پیاده سازی هرچه بهتره پروژه‌ها گروه‌های دانشجویی می‌توانند سه نفره نیز باشند، پس لازم است به نکاتی زیر توجه داشته باشید.

- پروژه‌ها به صورت بسته‌های چالش، شامل دو الی سه مسئله به گروه‌ها تخصیص داده می‌شود.
- برای ارسال پروژه‌ها(کد) سازوکاری در نظر گرفته شده است که طی اطلاعیه‌ای به اطلاع دانشجویان می‌رسد.
- برای ارسال گزارش‌های احتمالی هر گروه نیز سازوکاری برای دانشجویان در نظر گرفته شده است، که در ادامه به اطلاع دانشجویان می‌رسد.
- لطفا به تاریخ ارسال پروژه‌ها که در سامانه سامیا اطلاع رسانی می‌شود، دقت کنید.
- زمان بندی ارسال بسیار مهم است، پس لازم است به آن توجه شود.
- کپی برداری مستقیم از پروژه‌های موجود در سطح اینترنت مجاز نیست، در صورت مشاهده نمره منفی به همراه دارد. ایده برداری بلاملانع است.

موضوعات پروژه‌ها

بسته اول

۱. برنامه‌ای بنویسید که متنی را با استفاده از RSA به صورت رمز شده بین دو موجودیت انتقال دهید.

- کلاینت درخواست خود را برای گرفتن کلید عمومی از سرور،به سرور می‌فرستد.
- سرور اطلاعات مربوط به کلید عمومی خود $PU_{Server} = n_{Server}, e_{Server}$ را در پاسخ برای کلاینت ارسال می‌کند.
- کلاینت کلید عمومی خود را $PU_{Client} = n_{Client}, e_{Client}$ برای سرور ارسال می‌کند.
- کلاینت متن مورد نظر خود را (شماره دانشجویی) با استفاده از اطلاعات بدست آمده رمز می‌کند و برای سرور ارسال می‌کند.

- سرور نیز با اطلاعات بدست آمده، متن را رمزگشایی می‌کند

۲. حمله Side Channel بر روی AES در Lora را بررسی کنید.

۳. در مورد مراحل طراحی و توسعه یک الگوریتم رمزنگاری تحقیق کنید.

بسته دوم

۱. با استفاده از یک زبان برنامه نویسی، برنامه‌ای بنویسید که با استفاده از الگوریتم خاصی، بتواند دستگاه‌های فعال در یک شبکه محلی را شناسایی کند. همچنین بتواند پورت‌های باز هر دستگاه را شناسایی کند (بهینه بودن و سرعت برنامه در این مسئله مهم است).

۲. یک شبکه محلی را شبیه سازی کنید، که حمله Smurf بر روی آن در حال رخ دادن است. با استفاده از یک IDS به مانند Snort این حمله را تسخیص دهید.

۳. در مورد حملات پیشرفته APT تحقیق کنید و چند نمونه از این حملات را تشریح کنید.

بسته سوم

۱. برنامه‌ای بنوسید که بتواند کارهای زیر را انجام دهد.
- تشخیص وب سرور
- بدست آوردن محل سرور
- پورت‌های باز سرور
- ایمیل‌های به کار رفته در وب‌سایت را پیدا و ذخیره کند.

۲. یک شبکه محلی راه اندازی کنید و برای آن یک فایروال در نظر بگیرید، می توان از فایروال Pfsense استفاده کرد، فایروال را طوری تنظیم کنید که:
- وب‌سایت aparat.com را مسدود کند.
- از حمله DoS نیز جلوگیری کند.
- بتواند IP های مشکوک را تشخیص دهد.

۳. در مورد روش‌های پنهان‌نگاری متن در تصویر تحقیق کنید و یک نمونه انجام دهید.

بسته چهارم

۱. با استفاده از یک زبان برنامه نویسی WiFi Jammer طراحی کنید(سرعت عمل و بهینه بودن مهم است).

۲. شبکه‌ی محلی برای خود شبیه سازی کنید و برای آن یک HoneyPot در نظر بگیرید. می‌توانید برای این کار از Express-HoneyPot استفاده کنید. همچنین پیاده سازی سناریو استفاده از این HoneyPot را انجام دهید.

۳. در مورد روش‌های پنهان کردن یک بدافزار از دید آنتی ویروس‌ها تحقیق کنید و چند نمونه ابزار در این زمینه را ارزیابی کنید.

بسته پنجم

۱. با استفاده از یک زبان برنامه نویسی، TLS را پیاده سازی کنید و انواع پیاده سازی آن را بیاورید، هدف از حل این سوال صرفا آشنایی با چگونگی پیاده سازی TLS می‌باشد، و نیاز به پیاده سازی از پایه ندارد.

۲. در این سناریو می‌خواهیم یک حمله Directory Attack را داشته باشیم، همچنین با پیاده سازی یک HIDS به مانند OSSEC این حمله را در شبکه تشخیص دهیم.

۳. در مورد روش‌های شنود در شبکه تحقیق کنید و ابزارها آن را نام ببرید. یک نمونه حمله را تشریح کنید.

بسته ششم

۱. یک Web Crawling طراحی کنید! با استفاده از یک زبان برنامه نویسی دلخواه یک ابزار Web Crawlingطراحی کنید.

۲. حمله DNS Spoofing را در شبکه محلی خود پیاده سازی کنید و Snort را طوری تنظیم کنید که بتواند این حمله را تشخیص دهد.

۳. در مورد روش‌های تشخیص نفوذ و ابزارهای معروف Web Crawling و متدهای آن تحقیق کنید.

بسته هفتم

۱. با استفاده از یک زبان برنامه، برنامه‌ای بنویسید که با استفاده از الگوریتم ElGemal رشته‌ای از متن را بین دو موجودیت رمز کند، سپس رمزگشایی کند.

۲. با استفاده از ابزار Jadx یک برنامک اندروید را مهندسی معکوس کنید و تحلیل خود را در گزارش بیاورید.

۳. در مورد OWASP Top 10 2021 تحقیق کنید و موارد ریسک را در گزارش خود با توضیح بیاورید.

بسته هشتم

۱. برنامه‌ای بنویسید که ویژگی‌های زیر را دارا باشد.
   - الگوریتم AES را پیاده سازی کند
   - الگوریتم را تحلیل کند
   - طوری الگوریتم را توسعه دهید که آسیب پذیر شود.

۲. یک IPsec در شبکه محلی خود راه اندازی کنید.

۳. در مورد تحلیل رمز و ابزارهای آن تحقیق کنید.

بسته نهم

۱. با استفاده از یک زبان برنامه نویسی، یک Web Path Scannerطراحی کنید. می‌توان از ابزار CyberCrowl Scan نیز ایده برداری کنید.

۲. در شبکه محلی خود یک سناریو تست نفوذ به یک هدف ویندوزی را با استفاده از ابزار Metasploit پیاده سازی کنید.
۳. در مورد روش‌های تست نفوذ به ویندوز، ابزارهای ارایه شده و آسیب پذیری‌های آن تحقیق کنید.

بسته دهم

۱. یک ابزار ساده حمله DoS طراحی کنید، می‌توان برای ایده گرفتن از ابزارهای موجود استفاده کنید.
۲. در یک شبکه محلی سناریو فیشینگ را با استفاده از ابزارهای موجود پیاده سازی کنید.
۳. در مورد متدهای حمله از گروه DoS و DDoS تحقیق کنید و روش‌های جلوگیری را نیزشرح دهید.

بسته یازدهم

۱. ابزاری طراحی کنید که بتواند در یک شبکه محلی خزش کند و آسیب پذیری‌های رایج را تشخیص دهد، منظور از آسیب پذیری: پورت‌های بحرانی باز، آسیب پذیری در ورژن وب سرورها و همچنین نسخه PHP و دیتابیس می‌باشد.
۲. شبکه محلی را شبیه سازی کنید و آسیب پذیری‌های مربوط به سوال قبلی را در آن پیاده سازی و تست کنید.
۳. در مورد مکانیزم‌های نفوذ و آسیب پذیری‌های در سطح وب سرورها تحقیق کنید.

بسته دوازدهم

۱. ابزاری طراح کنید که بتواند گرافی از دستگاه‌های فعال در شبکه و ارتباط آن‌ها رسم کند. به عنوان نمونه ارتباط گره های پایانی با سوییچ‌های محلی تا هسته شبکه محلی.
۲. با کمک وب‌سایت Exploit-db یک نمونه از آسیب پذیری‌های سطح سیستم عامل را انتخاب کنید و سعی کنید در شبکه محلی خود از آن استفاده و پیاده سازی کنید.
۳. در مورد آسیب پذیری‌های سطح سیستم عامل به عنوان نمونه لینوکس‌ها و ویندوز تحقیق کنید، و متدهای استفاده شده در بهره‌وری از این آسیب پذیری‌ها را ذکر کنید، و در مورد آن توضیح دهید.

بسته سیزدهم

۱. وب‌سایتی آسیب پذیری SQL دارد، ابزاری طراحی کنید که بتواند این آسیب پذیری را کشف و SQL injectionانجام دهد، می‌توانید از ابزار SqlMap نمونه برداری کنید. برای تست ابزار خود می‌توانید از آزمایشگاه تست نفوذ رایگان DVWA استفاده کنید.
۲. ابزارهای تست نفوذ وب را بررسی کنید و یک سناریو در این سطح به دلخواه پیاده سازی کنید. می‌توانید برای پیاده سازی سناریو خود از DVWA استفاده کنید.
۳. در مورد تمام جوانب آسیب پذیری SQL و متدهای وقوع آن تحقیق کنید و راه‌های جلوگیری را نیز ذکر کنید.

بسته چهاردهم

۱. ابزاری طراحی کنید که بتواند با استفاده از ۵ الگوریتم، به صورت جدا متنی را رمز کند و رمزگشایی انجام دهد. سپس مقایسه‌ای از سرعت اجرای هر الگوریتم نیز داشته باشید، برنامه باید به طوری طراحی شود که مقایسه این الگوریتم‌ها در رمزنگاری و رمزگشایی را در خروجی داشته باشد. الگوریتم‌های مورد نظر:

- Triple Data Encryption Standard (TripleDES)
- Blowfish Encryption Algorithm
- Twofish Encryption Algorithm
- Advanced Encryption Standard (AES)
- IDEA Encryption Algorithm

۲. در مورد آسیب پذیری‌ها در سطح الگوریتم‌های رمزنگاری داده، مطالعه کنید و یک نمونه آن را پیاده سازی کنید.

۳. در مورد الگوریتم‌های سبک وزن رمزنگاری داده تحقیق کنید و در مورد نحوه پیاده سازی آن‌ها توضیح دهید.

بسته پانزدهم

۱. یک سیستم احراز اصالت با استفاده از الگوریتم ASCON طراحی کنید، در این سیستم، گره‌های پایانی باید احراز اصالت خود را به گره اصلی (Master Node) انجام دهند. پیاده سازی باید با یک زبان برنامه نویسی صورت بگیرد.

۲. در مورد الگوریتم‌های جدید احراز اصالت سبک وزن تحقیق کنید و روش پیاده سازی آن را با الگوریتم‌های پیشین مقایسه کنید.

بسته شانزدهم

۱. برنامه‌ای بنویسید که حمله Wiener را بر روی RSA پیاده سازی کند.

۲. ابزارهای رایج حمله به RSA را بررسی کنید و یک نمونه حمله با این نوع از ابزارها پیاده سازی کنید.

۳. در مورد حملهSide-Channel بر روی RSA تحقیق کنید و چگونگی آن را شرح دهید.

بسته هفدهم

۱. برنامه‌ای بنویسید که الگوریتم Elliptic Curve Cryptography را پیاده سازی کند، همچنین کاربرد آن در IoT را نیز به عنوان یک سناریو کاربردی بیان کنید.

۲. انواع حملات بر روی دستگاه‌های IoT را بررسی کنید و یک نمونه به دلخواه شبیه سازی کنید.

۳. در مورد روش‌های نوین احراز اصالت در IoT تحقیق کنید، و راه‌کارهای آن را ارایه دهید.

بسته هجدهم

۱. با استفاده از یک زبان برنامه نویسی برنامه‌ای بنویسید، که یک پیام رسان نظیر به نظیر را پیاده سازی کند، برای امنیت بالاتر پیام‌های رد و بدل شده از یک الگوریتم رمزنگاری مناسب استفاده کنید. پیام رسان شما باید حتما peer-to- decentralized peer باشد.

۲. نقاط ضعف و قوت پیام رسان‌های نظیر به نظیر را بیابید، همچنین سعی کنید چند نمونه از تهدیدهای این نمونه از شبکه‌ها را به تفکیک توضیح دهید.

۳. در مورد پیام رسان‌هایی که با این نوع از شبکه کار می‌کنند تحقیق کنید، و چند نمونه را بررسی دقیق کنید.

بسته نوزدهم

۱. برنامه‌ای بنویسید که با استفاده از آن بتوان حمله DoS را تشخیص داد، همچنین بتوان بهترین واکنش را به این حمله نشان داد.

۲. یک Keylogger طراحی کنید به طوری که بتواند Log کیبورد را در زمانبندی مشخصی به Email مشخصی ارسال کند.

۳. در مورد روش‌های تشخیص حمله‌ی DoS و DDoS که با استفاده از تکنیک‌های یادگیری ماشین رخ می‌دهد تحقیق کنید. و یک نمونه از پیاده‌سازی آن را تحلیل کنید.

بسته بیستم

۱. با استفاده از الگوریتم ISAP یک سیستم احراز اصالت طراحی کنید، به گونه‌ای که بین دو موجودیت بتواند با استفاده از این الگوریتم احراز اصالت بوجود آید و همچنین بعد از آن دیتایی بین این دو موجودیت رد و بدل شود.

۲. در مورد سیستم‌های احراز اصالت معروف تحقیق کنید و یک نمونه را پیاده سازی و راستی آزمایی کنید.

۳. یک سیستم احراز اصالت باید دارای چه ویژگی‌های باشد، د رمورد طراحی آن تحقیق کنید.

بسته بیست‌ویکم

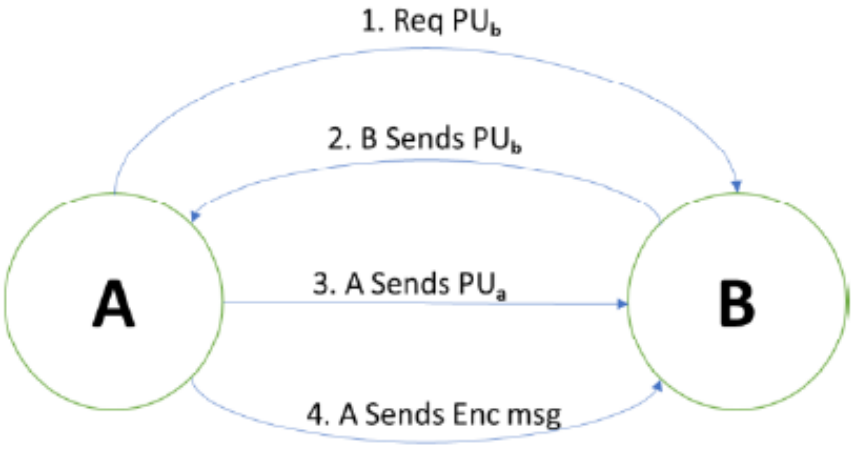
۱. برنامه‌ای بنوسید که بتواند یک وب‌سایت را به لحاظ آسیب پذیری‌ها بررسی کند و در صورت آسیب پذیر بودن، پیغامی مبنی بر آن آسیب پذیری خاص نمایش دهد. برای پیدا کردن آسیب پذیری‌ها و Exploitها می‌توانید از وب‌سایت‌های همچون Exploit-db استفاده کنید. حداقل ۱۵ آسیب پذیری باید در دیتابیس برنامه شما باشد.

۲. در مورد طراحی یک Exploit تحقیق کنید. همچنین مثالی در برنامه Exploit Pack نمایش دهید.

۳. در مورد Exploit نویسی و زبان‌های رایج استفاده شده برای آن تحقیق کنید.

بسته بیست‌ودوم

با استفاده از RSA میخواهیم متنی را بین دو موجودیت به صورت رمز شده انتقال دهیم. برای این کار مراحل زیر را طی نمایید:



شکل ۱: شمایی از اتصال کلاینت و سرور

ابتدا با استفاده از socket ارتباطی بین کلاینت و سرور خود ایجاد کنید. (لازم به ذکر است که در اینجا تفادتی بین سرور و کلاینت قائل نیستیم. صرفا کلاینت شروع کننده ارتباط است). هر یک از موجودیت‌ها کلید خصوصی(d)، عمومی (e) و پیمانه محاسبات(n) را در اختیار دارند. (برای تولید این مقادیر میتوانید از سوال قبل استفاده کنید. اعداد اول بزرگ نیاز نیست.)

ارتباط بدین صورت شکل می‌گیرد که:

۱. کلاینت درخواست خود را برای گرفتن کلید عمومی سرور برای سرور می‌فرستد.
۲. سرور اطلاعات مربوط به کلید عمومی خود را در پاسخ برای کلاینت ارسال می‌کند.
۳. کلاینت کلید عمومی خود را برای سرور ارسال می‌کند.
۴. کلاینت متن مورد نظر خود را (شماره دانشجویی) با استفاده از اطلاعات بدست آمده رمز می‌کند و برای سرور ارسال می‌کند.
۵. سرور نیز با اطلاعات بدست آمده متن را رمزگشایی می‌کند.

توجه: تمامی مراحل را به صورت گام به گام و کارهایی که در هر سمت صورت می‌گیرد را پرینت کنید. در انتها تصویری از ترمینال‌های سرور و کلاینت که حاوی تمامی اطلاعات مورد نیاز است را نیز در گزارش بیاورید.