به نام خدا

مدیریت و مهندسی امنیت

نیم‌سال دوم ۱۴۰۲-۱۴۰۱

دانشکدهٔ مهندسی کامپیوتر

دانشگاه صنعتی شریف

مدرس: **مهدی خرازی**

موضوع: **آشنایی با TPM و حذف امن**

موعد تحویل: **ساعت ۲۳:۵۹ ۲۸ اسفند ۱۴۰۱**

با سپاس از: **سیده عاطفه موسوی**

۱ مقدمه

هدف از این تمرین آشنایی عملی با TPM و موارد مربوط به حذف امن داده‌ها از روی سیستم است.

۲ TPM

۱. آیا کامپیوتر شما چیپ TMP دارد ؟ برند و مدل آن چیست ؟

۲. آیا چیپ TPM شما فعال است ؟ اگر فعال نیست آیا می‌توانید از bios آن را فعال کنید؟

۳. در این مرحله با یک سیستم دارای TPM کار کنید و سعی کنید با تنظیم TPM برای ضبط اندازه‌گیری چکیده مراحل بوت به سوالات زیر پاسخ دهید:

- تنظیم اولیه مربوط به TPM را چطور انجام داده اید (اگر به صورت خود به خود اندازه گیری صورت گرفته است و پیشفرض سیستم بوده است مسیر درست تنظیم آن را پیدا کرده و درج نمایید)
- چه تعداد اندازه گیری انجام شده است ؟ (چه تعداد کد/فایل چکیده گیری شده است)
- فایل های دخیل در مراحل بوت چه مواردی بوده اند و در کجا ذخیره شده اند و چکیده آنها در کدام رجیستر TPM بوده است؟
- اگر بخواهید دسته بندی روی فایل های دخیل در این عملیات انجام دهید چه دسته فایل هایی در این اندازه گیری در نظر گرفته شده اند؟
- مقادیر چکیده های اندازه گیری شده توسط TPM را از کجا خوانده اید و آیا محافظتی از آنان انجام شده بود؟ به نظر شما دلیل این امر چیست ؟

۱.۲ نکات

- اندازه گیری مراحل بوت می تواند مستقل از تنظیم بوت امن صورت گیرد تا از بروز مشکلات احتمالی جلوگیری کند بنابراین برای این تمرین اگر بوت امن سیستم فعال نیست نیازی نیست آن را فعال کنید و فقط با فعال سازی تی پی ام هم کار انجام می شود. در عین حال می توانید برای اطمینان با ماشین مجازی که تی پی ام آن فعال شده باشد کار کنید.
- اگر می‌خواهید بوت امن را فعال کنید ابتدا فرآیند کار را درک کنید تا داده‌های خود را از دست ندهید.

۳ حذف امن

۱. ابتدا نوع هارد دیسک(SSD/HDD) را مشخص کنید و آن را به همراه نام مدل و سازنده ذکر نمایید .

۲. برای اطمینان از عدم بروز اشتباهات احتمالی یک ماشین مجازی ایجاد کنید و بقیه مراحل را در ماشین مجازی (با هر سیستم عامل دلخواهی)انجام دهید.

۳. تحقیق کنید آیا محدودیتی برای داشتن هریک از انواع (ssd/hdd)در محیط های مجازی وجود دارد یا نه ؟ و آیا می توانید در ساخت دیسک روی یک ماشین با یک نوع دیسک (مثلا hdd) نوع دیگری را (مثلا SDD) به صورت مجازی ایجاد کنید؟ در نهایت لازم است نوع دیسک ماشین مجازی که ساختید را برای انجام قسمت های بعد نظر داشته باشید .

۴. سعی کنید یک Volume به نام test برای انجام این تمرین ایجاد کنید و در این درایور ۳ فایل به ترتیب با محتویات متنی (به عنوان نمونه فایل با پسوند txt.)محتویات تصویری (به عنوان نمونه فایل با پسوند jpg.) و محتویات برنامه ای (به عنوان نمونه فایل با پسوند exe.) قرار دهید

۵. درباره چگونگی پیاده سازی مفهوم clearing در راهنمای NIST 800-88 تحقیق کنید و در اینجا شرح دهید منظور از این مفهوم چیست و در تکنولوژی های مختلف هارد دیسک چه تفاوت هایی با هم دارد؟ همچنین مشخص کنید در نوع هارد دیسک شما این مفهوم چگونه پیاده سازی می شود؟

۶. حال محتویات test را یک بار با پاک کردن عادی (keyboard delete)و یک بار با توجه به مفهوم Clearing در سیستم پاک کنید(کد/دستورات استفاده شده کامل ضمیمه شود یا ارجاع مشخصی داده شود و از تمامی مراحل تصویر درج شود).

۷. با یک ابزار کشف شواهد رایانه ای تحقیق کنید آیا اطلاعات مورد نظر شما در هر حالت کامل پاک شده است یا هنوز داده هایی در این باره قابل بازیابی است؟

۸. مراحل ۳ تا ۷ را برای مفهوم Purge در راهنمای NIST 800-88 انجام دهید. درصورتیکه برای نوع هارددیسک/سیستم عامل خود در این مرحله محدودیتی یافتید این محدودیت را ذکرنمایید

۹. با توجه به اینکه شما در محیط مجازی حذف امن را انجام داده اید(و نه روی یک سیستم عامل غیر مجازی میزبان)به سوالات زیر پاسخ دهید:

- آیا اگر ناهمخوانی بین نوع دیسک مجازی و دیسک واقعی وجود داشته باشد مشکلی در حذف امن به وجود می آید یا خیر؟
- با در نظر گرفتن این نکته که حذف امن در سناریوهای ابری(که آن ها هم دارای محیط مجازی هستند) برای کاربران یک نگرانی جدی است آیا می توانید با مطالعه در این حوزه پارامترهای دیگری را بیابید که برای اطمینان از حذف امن در محیط های مجازی (اعم از کانتینرها یا ماشین های مجازی) در انواع سناریوهای خدمات ابری اهمیت دارند ؟

۴ تحویل‌دادنی‌ها

برای هر کدام از شما یک مخزن در طرشت با نام `ce876-012-your-student-id` ایجاد شده است. در صورتی که در طرشت حساب کاربری ندارید لطفا اطلاع دهید. شما باید گزارش نهایی خود را به فرمت Markdown ایجاد کنید و آن را با نام ce876-012-hw1-your-student-id.md در مخزن خود در طرشت قرار دهید. تمرین‌های ارسالی حتما باید حاوی عکس از مراحل کار شما باشد.

توجه داشته باشید که زمانی برای جلسه‌ی تحویل حضوری شما نیز در نظر گرفته خواهد شد.