به نام خدا

پروژه پایانی درس مهندسی نرم‌افزار

دانشکده‌ی مهندسی برق و کامپیوتر- دانشگاه صنعتی جندی شاپور دزفول

نیمسال دوم- سال تحصیلی ۹۹- ۱۳۹۸

- **عنوان پروژه:** طراحی و پیاده‌سازی یک جاسوس‌افزار[۱] در محیط یک شبکه‌ی محلی مجازی.

- **شرح پروژه:** دانشجویان بایستی در قالب گروه‌های حداقل ۲ و حداکثر ۴ نفره، پس از طرح ریزی[۲]، تجزیه و تحلیل و طراحی مدل جاسوس‌افزار به پیاده‌سازی آن به قرار زیر بپردازند.
(فازهای طرح‌ریزی و طراحی را دقیقاً شبیه به آن‌چه در پروژه‌ی درس تحلیل و طراحی سیستم‌ها گفته شد، انجام دهید؛ یعنی ایجاد یک سند[۳] چند صفحه‌ای از اهداف و نیازمندی‌های سیستم مورد طراحی(جاسوس‌افزار) به عنوان طرح‌ریزی پروژه، استفاده از نرم‌افزار Rational Rose جهت ترسیم نمودارهای UML (حداقل سه نمودار ترسیم شود) و سپس نوشتن سناریوهای مربوط به سیستم در قالب یک سند چندصفحه‌ای دیگر)

- **نیازمندی‌های پیاده‌سازی:** سیستم‌عامل ویندوز مایکروسافت(حداقل ویندوز ۷) و آشنایی با اصول و مبانی برنامه‌نویسی دسته‌ای[۴] که مقدماتی از آن در قالب دو جلسه‌ی عملی در آزمایشگاه شبکه دانشکده، تشریح و تبیین گردید. همچنین دارا بودن تسلط کافی بر دستورات و مفاهیم خط فرمان[۵] سیستم‌عامل ویندوز مایکروسافت. به منظور دریافت فیلم‌های آموزشی مفاهیم خط فرمان و برنامه نویسی دسته‌ای سیستم‌عامل ویندوز می‌توانید از پیوندهای زیر استفاده نمایید:

http://www.aparat.com/v/fh4JF
http://www.aparat.com/v/v8ZPu

تبصره: در صورت تمایل می‌توان پیاده‌سازی پروژه پایانی را با استفاده از سیستم‌عامل لینوکس و به تبع آن اصول کار با پایانه‌ی لینوکس[۶] و برنامه‌نویسی پوسته[۷] لینوکس انجام داد.

---

۱ Spyware
۲ Planning
۳ Document
۴ Batch Programming
۵ Command Prompt (CMD)
۶ Linux Terminal
۷ Shell Programming

❖ **تشریح محیط سیستم مورد نظر:** همان‌گونه که ذکر گردید، در این پروژه طراحی یک جاسوس‌افزار با ویژگی‌هایی که در ادامه ذکر خواهد شد مطلوب می‌باشد. به طور کلی، این جاسوس‌افزار وظیفه‌ی دریافت اطلاعات جامع سخت‌/نرم‌افزاری سیستم قربانی[۱](مورد هدف) را بر عهده دارد.

برای این‌منظور هر گروه بایستی، ابتدا با استفاده از نرم‌افزار قدرتمند VMWare Workstation اقدام به ساخت یک شبکه محلی[۲] متشکل از ۳ یا ۴ سیستم مجازی همگون با پلتفرم ویندوز(ترجیحاً ویندوز ۷) یا لینوکس (یکی از توزیع‌های پایدار شده[۳] دلخواه) نماید. سپس با استفاده از یک سوویچ مجازی، سیستم‌های مجازی مذکور را به سیستم فیزیکی که برنامه‌ی جاسوس‌افزار روی آن نوشته شده متصل نموده و منابع مورد نیاز را به اشتراک گذارند.

پس از تکمیل پیاده‌سازی پروژه جاسوس‌افزار، فایل دسته‌ای آن را یا درقالب فایلی با پسوند bat. و یا یک فایل اجرایی مورد استفاده ویندوز (exe.)، از طریق شبکه‌ی ایجادشده با استفاده از نرم‌افزار VMWare Workstation میان ۳ یا ۴ سیستم مجازی به اشتراک گذارده و در هریک اجرا نمایند. سپس نتیجه حاصل از خروجی اجرای جاسوس‌افزار را در یک فایل متنی[۴] ثبت[۵] نموده و در اختیار سیستم فیزیکی مهاجم[۶] قرار دهند. توجه کنید که به منظور ارتباط میان سیستم فیزیکی (مهاجم) و سیستم‌های قربانی، دو روش کلی وجود دارد:

الف) ایجاد یکی از انواع فایل‌های bat. یا exe. و اشتراک‌گذاری دستی آن‌ها برای سیستم‌های قربانی. سپس ورود به هریک از سیستم‌های قربانی و اجرای فایل به اشتراک‌گذارده شده به صورت دستی و انتقال فایل متنی ثبت وقایع به صورت دستی به سیستم فیزیکی مهاجم (نمره‌ی اضافی *نداشته* و مسیر *اجرای عمومی* پروژه است).

ب) نوشتن یک دست‌نویس[۷] با قابلیت اجرای فرامین از راه دور[۸] توسط سیستم فیزیکی مهاجم؛ به قسمی‌که پس از اشتراک‌گذاری فایل bat. یا exe.، به طور خودکار این فایل را در تک‌تک سیستم‌های قربانی اجرا نموده و فایل متنی ثبت وقایع[۹] را به سیستم مهاجم فیزیکی ارسال نماید (دارای نمره‌ی اضافی *قابل توجه* بوده و به عنوان یک مسیر *خلاقانه* در پیاده‌سازی پروژه در نظر گرفته می‌شود).

---

۱ Victim System
۲ Local Area Network (LAN)
۳ Stable Distributions
۴ Text File
۵ Log
۶ Attacker Physical System
۷ Script
۸ Remote Command Execution
۹ Log Text File

❖ **ملزومات جاسوس‌افزار مورد طراحی:** هر گروه بایستی به عنوان اساسی‌ترین ملزومات یک جاسوس‌افزار، اطلاعات مهم زیر را از سیستم‌های قربانی به یکی از دو روش مزبور، دریافت نماید. همچنین به منظور اخذ نمره‌ی اضافی، هر گروه می‌تواند با هر نوع روش خلاقانه، جاسوس‌افزار مورد طراحی خود را به یک تروجان نیز تبدیل نماید (به عنوان نمونه، فایل اجرایی جاسوس‌افزار مورد نظر را درون یک فایل تصویری مانند jpg. یا bmp.، PNG. و ... جاسازی(تعبیه)[1] نماید). ملزومات مذکور به شرح زیر می‌باشند:

۱- **دریافت اطلاعات مربوط به خود سیستم عامل از قبیل: نام سیستم عامل – نسخه آن – زمان محلی سیستم عامل (تاریخ و ساعت) – نوع سیستم عامل (X86/X64)**

۲- **دریافت اطلاعات مربوط به سخت افزار کامپیوتر: نام Motherboard – کمپانی سازنده Motherboard – نسخه BIOS – نام هارد دیسک – حجم هارد دیسک – سریال هارد دیسک – نام کارت شبکه – سرعت کارت شبکه – نام CD/DVD ROM – نام CPU – تعداد هسته های CPU – نام RAM – حجم RAM – نوع RAM – نام گرافیک – حجم گرافیک – نوع گرافیک**

۳- **بررسی اطلاعات مربوط به کاربر: نام کامپیوتر (Hostname) – نام حساب کاربری (Username) – مسیر پروفایل حساب کاربری – تعداد پارتیشن های هارد دیسک – بررسی فایلهای شخصی کاربر – بررسی جستجوهای انجام شده توسط کاربر – مرورگر های مورد استفاده کاربر – نرم افزار های مورد استفاده کاربر**

۴- **بررسی امنیت سیستم عامل: آیا آنتی ویروس نصب و فعال روی سیستم عامل وجود دارد؟ – آیا فایروال نصب و فعال وجود دارد؟ – آیا فایروال خود سیستم عامل فعال است؟ – آیا کاربر روی حساب کاربری خود رمز گذاشته؟ – آیا حساب کاربری کاربر Standard است یا Administrator ؟ – آیا UAC ویندوز فعال است یا خیر؟ – آیا سرویس Windows Update فعال است یا خیر؟ آیا کاربر از سرویس های خاص مثل Telnet یا SSH استفاده میکند؟**

توجه کنید که به منظور پیاده‌سازی جاسوس‌افزار مورد نظر، لازم است اهداف چهارگانه‌ی زیر در کدنویسی برنامه، مورد توجه قرار گیرد:

هدف اول: دریافت اطلاعات سیستم‌عامل قربانی

هدف دوم: دریافت اطلاعات سخت‌افزاری سیستم قربانی

هدف سوم: دریافت اطلاعات مربوط به کاربران سیستم قربانی

هدف چهارم: بررسی امنیت سیستم عامل سیستم قربانی

❊ در صورت انتخاب هر یک از دو روش مزبور، لازم است از کلیه‌ی مراحل انجام شده عکس گرفته شود[2] و در قالب یک سند MSWORD به همراه توضیحات هر مرحله، درج شود. سپس این فایل به همراه کد یا

---

[1] Embed

[2] Screen Shot

اسکریپت نوشته شده(یک یا چند فایل txt.)، به علاوه‌ی مجموعه فایل‌های مربوط به فازهای طرح‌ریزی و طراحی، همگی در یک پوشه قرار داده شده و پوشه‌ی مورد نظر، فشرده‌سازی[1] شود.

نحوه‌ی نام‌گذاری پوشه(فایل فشرده‌سازی شده) به صورت زیر است:

<JSU>_<SE>_<GroupNO>_<FinalProject>

مثلاً برای گروه شماره ۳ داریم:

JSU_SE_Group3_FinalProject

پس از تعیین اعضای هر گروه، یک نفر به نمایندگی از سایر اعضا، به بنده ایمیل داده و اعضای گروه را مشخص می‌نماید. پس از دریافت اسامی کلیه‌ی اعضای گروه‌ها، به هر گروه یک شماره تخصیص داده می‌شود که این شماره‌ها در سامانه قرار خواهد گرفت و براساس آن هر گروه می‌تواند فعالیت‌هایی نظیر نام‌گذاری پوشه‌ی خود را انجام دهد.

آدرس ایمیل بنده و قالب موضوع ایمیل ارسالی از طرف نماینده هر گروه، به صورت زیر است:

Email Address: promotion.academy12@gmail.com
Your Email Subject: JSU_SE_GroupMembers

حداکثر مهلت تعیین اعضای گروه‌ها: ۹۹/۰۳/۱۹

(هرگونه تاخیر در ارسال و تعیین اعضای گروه‌ها مشمول کسر نمره خواهد شد)

موفق و پیروز باشید- امین عنایت زارع

[1] Zip(Compressed)