Gاهداف پروژه:

شروع: در اصل هدف از انجام پروژه!

استخراج داده از کامپیوتر و ارسال به کامپیوتر مهاجم، دریافت اطلاعات از کامپیوتر مورد حمله.

اهداف :

هدف از ایجاد این جاسوس‌افزار، دریافت اطلاعات جامع سخت‌افزاری و {نرم‌افزاری} از سیستم قربانی می‌باشد.

اطلاعاتی که از سیستم قربانی بدست می‌آوریم :

## اطلاعات مربوط به سیستم عامل

نوع سیستم‌عامل

نسخه‌ی سیستم‌عامل

زمان محلی سیستم‌عامل

نام سیستم‌عامل

## اطلاعات مربوط به سخت‌افزار

نام Motherboard(مادربرد)

نام کمپانی سازنده مادربرد

نسخه BIOS (بایوس)

نام هارد دیسک

حجم هارد دیسک

سریال هارد دیسک

نام کارت شبکه

سرعت کارت شبکه

نام CD/DVD ROM

نام CPU (پردازنده)

تعداد هسته‌های CPU

نام RAM

حجم RAM

نوع RAM

نام گرافیک

حجم گرافیک

نوع گرافیک

## اطلاعات مربوط به کاربر

نام کامپیوتر

نام حساب کاربری

مسیر پروفایل حساب کاربری

تعداد پارتیشن‌های هارد دیسک

بررسی فایل‌های شخصی کاربر

بررسی جستجوهای انجام‌شده توسط کاربر

مرورگرهای مورد استفاده کاربر

نرم‌افزارهای مورد استفاده‌ی کاربر

## اطلاعات مروبط به امنیت سیستم‌عامل

نوع و وضعیت آنتی‌ویروس نصب شده

وضعیت فایروال

بررسی وجود گذرواژه برای حساب کاربری

نوع حساب کاربری (استاندارد/ادمین)

## وضعیت UAC ویندوز

وضعیت سرویس windows update

وضعیت استفاده از Telnet و SSH

# نحوه‌ی کار برنامه:

یک نسخه از فایل برنامه بر روی سیستم مورد حمله بارگذاری می‌شود که در صورت اجرا عملیات جمع‌آوری داده‌ها و ارسال آن‌ها روی بستر شبکه را انجام خواهد داد.

همچنین یک نسخه از برنامه بر روی سیستم حمله کننده وجود دارد که عملیات دریافت فایل داده‌ها از سیستم‌های مورد حمله روی بستر شبکه و نمایش فایل‌ها به کاربر حمله کننده بر عهده‌ی آن است.

شرح کار:

ایجاد شبکه بین چند سیستم و جاسوسی از آنها

برای تحقق هدف فوق نیازمندیهایی داریم که به شرح زیر است:

* نیاز به بیشتر از یک سیستم که بهم متصل شوند
* نیاز به وسایلی جهت انجام این اتصال (هاب، سوییچ، کابل LAN و ...)