طرح پیشنهادی

# نفوذ به شرکت های فعال مهندسی پزشکی

خرداد ماه ۱۴۰۳

## نسخه ۱.۰

# فهرست

## مقدمه

امروزه رشته مهندسی پزشکی و پیوندی که در بین علوم رشته‌های مهندسی و پزشکی ایجاد شده است باعث رشد بهره‌وری در حوزه‌های سلامت و اقتصادی شده است. به طوری که استفاده از دانش مهندسی در حل مشکلات و بهبود عملکرد تجهیزات و صنایع پزشکی و قرار گرفتن در لبه تکنولوژی در این حوزه به طور مستقیم در برخی از مؤلفه‌های قدرت یک کشور تأثیرگذار می‌باشد.

دو مفهوم شبیه به یکدیگر با عناوین بیوتکنولوژی (Biotechnology) و مهندسی پزشکی ( Biomedical Engineering) وجود دارد. تعاریف و تفاوت این دو حوزه با یکدیگر در ادامه تشریح شده است.

حوزه بیوتکنولوژی در ارتباط با بهبود زندگی انسان با استفاده از ترکیب دانش و فناوری با علوم موجودات زنده، سلول‌ها و سیستم‌های بیولوژی می‌باشد. بیوتکنولوژی با ترکیب اصولی از زیست‌شناسی، فیزیک، شیمی، ریاضیات و فناوری در جهت اهدافی مانند افزایش طول عمر انسان، افزایش بازدهی محصولات کشاورزی، کاهش گازهای گلخانه‌ای و در حوزه‌هایی مانند مراقبت‌های پزشکی، کشاورزی، داروسازی و حفاظت از محیط زیست مطرح شده و بکار گرفته می‌شود. در این حوزه نیز برخی موضوعات امنیتی مانند ترورهای بیولوژیکی، مواد غذایی تراریخته با هدف دستکاری ژنتیک و ساخت ویروس‌هایی هدفمند با جامعه هدف مشخص مطرح هستند.

از سوی دیگر مهندسی پزشکی یک رشته تخصصی در مهندسی است که شکاف بین اصول مهندسی و رشته پزشکی را پر می‌کند. در این زمینه می‌توان به دستگاه‌ها، ابزارها و روش‌های نوآورانه‌ای مانند انواع پروتز، فناوری‌های تصویربرداری، فناوری هسته‌ای و کاربرد آن در صنعت پزشکی، تجهیزات حفاظتی و استراتژی در زمینه پیشگیری از آسیب‌ها اشاره نمود. در واقع متخصصین این حوزه با استفاده از علم مهندسی برق، مکانیک، کامپیوتر و موارد مشابه سعی می‌کنند تا نتایج علم پزشکی را با بهره‌وری بالاتری ارائه کنند. این اتفاق می‌تواند در ارائه یک دستگاه پیشرفته بر گرفته از توان علوم فیزیک هسته‌ای در جهت درمان سرطان و یا پرتو درمانی باشد، یا ساخت ابزارهای ساده با هدف محافظت و پیشگیری از آسیب‌دیدگی‌ها.

با توجه به مقدمه مطرح شده درمورد اهمیت و چیستی دو مفهوم بیوتکنولوژی و مهندسی پزشکی، تمرکز ما در این پروژه بر روی تارگت‌هایی که در حوزه مهندسی پزشکی فعالیت دارند خواهد بود.

## مراحل پروژه

**مرحله اول: OSINT و جمع آوری اطلاعات اولیه**

این مرحله در حاضر تا ۲۰ درصد انجام شده است و لیست ۳ شرکت فعال و برتر در این حوزه مشخص شده است. ۱۵ شرکت در مجموع در فاز اول OSINT تحت بررسی اولیه قرار خواهند گرفت.

در این مرحله اطلاعات زیر استخراج خواهد شد:

- نام شرکت
- اطلاعات اولیه:
  - نوع مالکیت
  - ارزش شرکت
  - حوزه فعالیت
  - آدرس دفاتر
  - نام مدیرعامل
  - اعضای اصلی شرکت
  - آدرس دامنه اصلی

برای اجرای این بخش ۲ نفر و در مجموع ۳۲ ساعت

نفرات:

- علی
- کوروش

اهداف:

- شناخت اولیه شرکت های دیگر
- تکمیل و گسترش اهداف

**مرحله دوم: Recon و پایش فعال و غیرفعال**

در این مرحله با هدف تکمیل داده ها برای اجرای ۳ سناریو حمله (فاز Initial Access) در نظر گرفته شده است.

سناریوهای حمله عبارتند از:

1- Exploit Public Facing Asset

2- Spread Phishing

3- Personnel Phishing

به منظور آماده سازی برای اجرای حمله ۱ داده های زیر نیاز است:

۱- لیست دامنه ها و زیردامنه ها به صورت دقیق
۲- لیست سرویس های فعال در گستره اینترنت
۳- رنج آیپی سازمان هدف

برای اجرای این مرحله ۲ نفر و در مجموع ۴۰ ساعت زمان در نظر گرفته شده است.

نفرات:

- حسام
- محمد

به منظور آماده سازی برای حمله ۲ مراحل زیر باید انجام شود:

۱- جمع آوری اطلاعات اشخاص فعال در سازمان + سمت (طراحی چارت سازمانی)
۲- تشخیص واحد کاری و نحوه کار (دورکاری یا حضوری)
۳- محل اشتغال (دفتر مرکزی؟ یا دفاتر جداگانه)
۴- آدرس های ایمیل اشخاص
۵- حساب های کاربری در فضای مجازی (Telegram, whatsapp, Instagram, ...)

برای اجرای این مرحله ۲ نفر و در مجموع ۳۰ ساعت زمان در نظر گرفته شده است.

نفر ات:

- علی
- کوروش

با توجه به داده های استخراج شده سناریوهای مختلف برای هر بخش طراحی خواهد شد.

اما به صورت کلی برای ارسال ایمیل فیشینگ در ابتدا باید داده های زیر بررسی شود:

۱- آیا امکان ارسال ایمیل Spoof وجود دارد؟

۲- در صورت وجود امکان ارسال ایمیل Spoof، روش وسوسه برای اجرای فایل چیست؟

۳- آماده سازی زیر ساخت از قبیل:

a. فایل آلوده winrar (آماده سازی rat جهت استفاده)
b. فایل آلوده word, excel, pdf

برای انجام اینکار ۲ نفر و در مجموع ۱۶ ساعت زمان در نظر گرفته شده است.

نفرات:

- شایان
- پرهام

این طرح تا مرحله قبل از initial Access میباشد. و با توجه به هر تارگت به صورت جداگانه طرح و زمان بندی مدنظر اعلام خواهد شد.

به پیوست سند OSINT انجام شده (نسخه اولیه) ارسال خواهد شد.

## خلاصه

به طور کلی اهداف در جدول زیر مطرح شده است.

| مرحله | نفر | ساعت تخمین زده شده |
|---|---|---|
| **OSINT** | علی<br>کوروش | ۳۲ ساعت |
| **Recon** | حسام<br>محمد | ۴۰ ساعت |
| **جمع آوری اطلاعات** | علی<br>کوروش | ۳۰ ساعت |
| **زیرساخت فیشینگ** | شایان<br>پرهام | ۱۶ ساعت |