پژوهشگاه نیرو	**فرم تشریح پروژه** **CoRFP20-3**	شرکت توانیر

عنوان پروژه:	**طراحی و پیاده‌سازی هانی‌پات صنعتی با قابلیت پشتیبانی پروتکل DLMS**
عنوان طرح:	**توسعه فناوری‌های امنیتی در صنعت برق**
واحد اجرایی:	**مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق**

برآورد کلی مدت زمان اجرای پروژه: 12 ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

در سالهای اخیر پیچیدگی و تنوع حمله‌های کامپیوتری افزایش قابل توجهی داشته‌اند. سازمانها عموماً از تجهیزات امنیتی رایجی مانند دیواره آتش و سیستم‌های تشخیص نفوذ برای مقابله با این حمله‌ها استفاده می‌کنند. این گونه تجهیزات امنیتی، محدودیت‌های بسیاری دارند و قادر به کشف تمام حمله‌های جدید و پیچیده نیستند. با توجه به ضعف تجهیزات امنیتی فعلی برای کشف حمله‌های ناشناخته و پیچیده، نیاز است که از راهکارهای دیگری برای شناسایی این تهدیدات استفاده شود. یکی از این راهکارها، استفاده از سیستم هانی‌پات است که در سالهای اخیر به یکی از مهمترین اجزای مراکز عملیات امنیت (***SOC***) و معماری امنیت شبکه سازمانها تبدیل شده است. هانی‌پات یک سیستم امنیتی است که بر خلاف سیستم‌های امنیتی دیگر، ارزش آن در کشف شدن، مورد حمله قرار گرفتن و به خطر افتادن است. بسته به نیاز سازمان، از هانی‌پات می‌توان برای مقاصد مختلفی از جمله شناسایی حمله‌ها و فعالیت‌های غیرمجاز در شبکه، کشف و جمع‌آوری بدافزار، فریب‌دادن نفوذگر و کندکردن روند حمله استفاده کرد.

اساس کار هانی‌پات مبتنی بر فریب دادن نفوذگر یا ***Deception*** است. در واقع با استفاده از هانی‌پات، با در معرض خطر قراردادن یک یا چند سیستم آسیب‌پذیر یا به ظاهر آسیب‌پذیر (شبیه‌سازی شده)، منتظر حمله به این سیستم‌ها شده و هر گونه فعالیتی بر روی آنها به عنوان عملی مشکوک یا حمله در نظر گرفته می‌شود. از آنجا که هانی‌پات هیچ کاربرد عملیاتی در سازمان ندارد، هر فعالیتی که بر روی آن انجام شود و یا هر ترافیک ورودی و خروجی از آن می‌تواند نشان‌دهنده حمله باشد. از این رو، هانی‌پات‌ها تشخیص غلط یا ***False Positive*** بسیار کمتری نسبت به سیستم‌های کشف نفوذ (***IDS***) دارند.

هانی‌پات دسته‌ای از سیستم‌های تشخیص نفوذ است که رویکردی کاملاً متفاوت از سیستم‌های تشخیص نفوذ سنتی دارد و بر خلاف آنها، نیازی به استفاده از امضاء حملات شناخته شده برای کشف ندارد. البته هانی‌پات را نمی توان جایگزین سیستم‌های تشخیص نفوذ سنتی در نظر گرفت. هانی‌پات سیستمی است که بر اساس تعریفش، فقط نفوذگر باید به آن دسترسی داشته باشد و ترافیک سیستم‌های عادی نباید به سمت آن هدایت شود. استفاده از این رویکرد، مشکل شناسایی حمله را ساده می‌کند. هانی‌پات ذاتاً نرخ تشخیص غلط (***false positive***) بسیار پایینی دارد و این یکی از مزایای اصلی هانی‌پات نسبت به سیستم‌های تشخیص نفوذ است. در مقابل، هانی‌پات نمی‌تواند حملاتی که مستقیماً به سیستم‌های عملیاتی سازمان انجام می‌شود (به هانی‌پات هدایت نمی‌شود) را شناسایی و از وقوع آنها جلوگیری کند. یکی دیگر از مزایای هانی‌پات، حجم کم لاگهای تولید شده و سهولت تحلیل آنها در مقایسه با سیستم‌های تشخیص نفوذ است. هانی‌پات و سیستم‌های تشخیص/جلوگیری از نفوذ، تکنولوژی‌های مکمل هم هستند: هانی‌پات می‌تواند قسمتی از حملاتی که توسط سیستم تشخیص نفوذ شناسایی نشده را کشف یا حداقل نشانه‌ای از آنها ثبت کند.

از طرف دیگر بدون شک زیرساخت‌های مربوط به صنایع مختلف از جمله صنعت نفت، گاز، پتروشیمی، آب، برق و نیروگاه‌ها جزء حساس‌ترین زیرساخت‌های هر کشور محسوب می‌شوند. در میان میان صنعت برق به عنوان زیرساختی که دیگر صنایع برای انجام فعالیت‌های خود به آن وابسته می‌باشند دارای اهمیت بسزایی است.

در این صنعت همانند دیگر صنایع به منظور خودکارسازی فرآیندها، کنترل و پایش آن‌ها از سیستم‌های کنترل صنعتی (***ICS***) استفاده می‌شود. متأسفانه اکثر سیستم‌های کنترل صنعتی بدون در نظر گرفتن موارد امنیتی توسعه یافته‌اند و به همین دلیل دارای آسیب‌پذیری‌های ناشناخته (***Zero-day***) و ضعف‌های امنیتی بسیاری هستند. به دلیل حساسیت زیاد زیرساخت‌های صنعتی، در سال‌های اخیر حملات و بدافزارهای بسیاری این سیستم‌ها را مورد هدف قرار داده‌اند. از این میان می‌توان به بدافزار پیچیده ***Stuxnet*** که یکی از اهدافش ایجاد اختلال در تأسیسات هسته‌ای کشورمان بود اشاره کرد.

بر خلاف تفکر رایج که ایزوله کردن و قطع ارتباط شبکه صنعتی از اینترنت را به تنهایی راهکار امنیتی کامل و بدون نقصی می‌داند، حملات مشاهده شده در سال‌های اخیر ضعف این رویکرد و امکان نفوذ به آن را اثبات کرده است. یکی از راهکارهای تکمیلی برای کشف حمله در شبکه‌های کنترل صنعتی، استفاده از هانی‌پات است. هانی‌پات صنعتی به صورت منفعل و بدون نیاز به تغییر پیکربندی سیستم‌ها در شبکه صنعتی قرار گرفته و سرویس‌های مرتبط با سیستم‌های کنترل صنعتی را به منظور کشف حمله در معرض تعامل با نفوذگر قرار می‌دهد. با استفاده از این سیستم امنیتی می‌توان فعالیت بدافزار یا نفوذگر را در شبکه کنترل صنعتی شناسایی و پیگیری کرد.

در این پروژه، هدف طراحی، ساخت و راه‌اندازی هانی‌پات صنعتی مناسب با صنعت برق می‌باشد که در وهله‌ی اول حملات شناخته و ناشناخته توسط مهاجمان را شناسایی نموده و همچنین با کسب اطلاعات به عنوان یک منبع آموزشی برای یادگیری روش‌های نفوذ به این صنعت مورد استفاده قرار گیرد. ولی با توجه به گستردگی حوزه کاری صنعت برق لازم است که طراحی این هانی‌پات صنعتی در طی فازهای مختلفی صورت گیرد. در این فاز پروژه با توجه به اهمیت فراسامانه هوشمند ***AMI*** به عنوان یکی از زیرساخت‌های مهم صنعت برق جهت مدیریت و پایش انرژی الکتریکی کشور، طراحی، ساخت و راه‌اندازی هانی‌پات صنعتی مد نظر است که قادر به شبیه‌سازی پروتکل ***DLMS*** به عنوان پروتکل اصلی این فراسامانه هوشمند باشد.

فازهای پیشنهادی جهت انجام این پروژه به شرح زیر می‌باشد:

- فاز اول- شناخت حوزه‌ی پروژه و تحلیل نیازمندی‌های مورد نیاز برای راه اندازی هانی‌پات صنعتی ***DLMS***
- فاز دوم– طراحی محصول با توجه به نیازمندی‌ها
- فاز سوم – پیاده‌سازی محصول
- فاز چهارم – تست کارکرد و یکپارچه‌سازی محصول

مشخصات محصول نهایی(خروجی مورد انتظار) :

- پشتیبانی از معماری توزیع شده (دارای یک سنسور و یک سرور مدیریت)
- شبیه‌سازی سرویس ***DLMS*** تا سطح ***2***
- گزارش‌گیری گرافیکی
  - ارائه داشبوردهای گرافیکی مناسب
  - استفاده از نقشه اختصاصی برای نمایش آدرس مهاجمین روی نقشه
  - ارائه دیاگرام وضعیت حملات صورت گرفته به شبکه تحت حفاظت
  - امکان ذخیره قالب گزارش به ازای هر کاربر(هر کاربر می‌تواند قالب‌های اختصاصی خودش را تعریف نماید.)

- تولید گزارشات متنوع
  - تعداد حملات شناسایی مبتنی بر هر سنسور
  - بالاترین آدرس‌های ***IP*** حمله‌کننده
  - بالاترین کشورهای حمله کننده
  - نمایش حملات بر اساس شماره پورت‌ها
  - تراکم حملات بر اساس بازه‌های زمانی مختلف
- نمایش وضعیت منابع(حافظه، پردازنده و ...) سامانه به صورت گرافیکی
- قابلیت ارسال بدافزارهای شناسایی شده به سیستم‌های تحلیل بدافزار برای انجام تحلیل بیشتر روی بدافزار
- در اختیار قرار دادن مکانیزم‌هایی برای قرار دادن رد حمله در کامپیوتر مهاجم و استفاده از آن در ***Forensics***
- دارای واسط کاربری گرافیکی تحت، برای دسترسی و پیکربندی آسان محصول از هر نقطه از شبکه
- ارسال بلادرنگ فایل‌های بدافزارها و ترافیک حملات شناسایی شده از سنسور به سرور مدیریت
- قابلیت تعریف دسترسی برای کاربران سامانه
- قابلیت ارسال تهدیدات و حملات شناسایی شده به سیستم‌های مدیریت لاگ برای کمک به تحلیل بهتر آن‌ها
- امکان شناسایی و جمع‌آوری اطلاعات زیر:
  - اطلاعات مهاجمین مانند آدرس ***IP*** مهاجم، کشور، شماره پورت، زمان حمله و ...
  - اطلاعات ارتباط مانند پروتکل مورد استفاده.
  - اطلاعات بدافزار مانند آدرس مکان دانلود و فایل بدافزار.
  - اطلاعاتی در مورد ابزارهای بکار گرفته شده توسط مهاجم مانند نام اسکنر مورد استفاده یا نام مرورگر استفاده شده
- امکان نمایش بلادرنگ تهدیدات شناسایی شده و قابلیت جستجو در آن‌ها
- ارسال بلادرنگ تهدیدات و حملات شناسایی شده توسط سنسورها به سنسور مدیریت
- امکان نمایش لیست بدافزاراهای ذخیره شده و تفکیک آن‌ها بر اساس نوع(بدافزارهای تکراری را می‌توان در یک گروه مشاهده نمود)
- تولید گزارشات متنوع بر اساس پارامترهای مختلف
- تولید گزارشات تهدیدات و حملات شناسایی شده به فرمت‌های مختلف مانند ***pdf***، ***html***
- امکان پیکربندی از راه دور محصول(سرور مدیریت و سنسورها) توسط پروتکل امن ***SSH***