امنیت شبکه های کنترل صنعتی

امین یونسی سینکی

۱۳۹۵

فهرست مطالب

بسم الله الرحمن الرحیم

مقدمه

بی شک ظهور سامانه های صنعتی از جمله DCSو SCADA و اتصال آن به شبکه جهانی،تأثیر شگرفی در توسعه فرآیندهای کنترلی زیرساخت های حیاتی کشورها، به ویژه نظارت وکنترل تجهیزات از راه دور داشته است . هرچند این پیشرفت و توسعه، آسیب پذیری های جدیدی را نیز به همراه داشته که امنیت سایبری سامانه های کنترل صنعتی را به چالش کشیده است .از این منظر شناخت کامل بسترها و بخش های آسیب پذیر و همچنین تهدیدات ناشی از آ ن ها امری لازم و ضروری است .پس از شناخت بخش های آسیبپذیری سامانه های صنعتی،بررسی راهکارهای تدافعی و بهبود سطح ایمنی، اقدماتی است که در کاهش تهدیدات و خطرات احتمالی نقش بسزایی دارد .ازجمله مهم ترین این اقدامات می توان به بهره گیری ازاستانداردها و توصیه نامه های ارتقای امنیت سایبری اشاره کرد.

طرح کلی امنیت سیستمهای کنترل صنعتی می تواند به عنوان مبنای کار در خصوص امنیت اینگونه سیستمها مد نظر قرار گرفته شود.

امین یونسی سینکی

کارشناس ارشد مکاترونیک(سیستمهای هوشمند)، کارشناس مهندسی کامپیوتر، کارشناس فیزیک

Amin_unesi@yahoo.com

Instagram: NETWORK.SECURITY

تعاریف واصطلاحات

:ICS

Industrial Control Network

:IT

Information Technology

:SCADA

Supervisory Control and Data Acquisition

:DCS

Distributed Control System

:PLC

Programmable Logic Controller

:Server

ایستگاهی در شبکه که سرویسهایی را برای سرویس گیرنده ها فراهم می کند.

:Protocol

قوانینی که برای تبادل اطلاعات بین دو شیء (سیستمهای شبکه ، برنامه های کاربردی) وجود دارد.

:IPS

مخفف Intrusion Prevention System معرف سیستم حفاظتی است که از خرابکاری های در حال وقوع بر روی شبکه جلوگیری می کند.

:IDS

مخفف Intrusion Detection System و خرابکاری های در حال وقوع بر روی شبکه را شناسایی می کند.

:DOS

Denial Of Service (Attack)

:IP

مخفف Internet Protocol وپروتکل پایه TCP/IP می باشد که برای حمل UDP،TCP و بسیاری از پروتکلهای سطح بالا بکار می رود.

تعریف سیستم های کنترل صنعتی:

سیستم های کنترل صنعتی ICS در حالت معمولی شامل انواع مختلف سیستم های کنترلی، از جمله سیستمهای کنترل سرپرستی و گردآوری داده ، سیستم های کنترلی توزیع شده و کنترل کننده قابل برنامه ریزی منطقی می شود .سیستم های به صورت گسترده در نیروگاه های اتمی، نیروگاه های برق، شبکه های توزیع الکتریسته، نفت و سیستم های گاز و همچنین حمل و نقل، صنایع دفاعی، جمع آوری زباله و حتی تولید خودرو مورد استفاده قرار می گیرد .سیستم های ICS سیستم هایی هستند که برای انجام وظایف خود نیازی به یک اپراتور انسان ندارند .در برخی از انواع که شبکه کنترلی مجزا شده فیزیکی دارند که سیستم را مجبور به برقراری ارتباط از طریق یک شبکه به دیگر ایستگاه های کنترلی می کند.

در سیستم های کنترل صنعتی دو مولفه مهم وجود دارد که عملکرد آنها به هم دیگر مرتبط است، این دو مولفه سیستمهای اسکادا و کنترل کننده های برنامه پذیر منطقی هستند .سیستم های اسکادا به منظور ارائه کردن اطلاعات به صورت بلادرنگ به یک اپراتور انسانی طراحی شده اند و می توانند اطلاعات حالت جاری فرآیندهای فیزیکی و همچنین توانایی تغییر ایجاد کردن در فرآیند از راه دور را به اپراتور ارائه کنند.سیستم های اسکادا امروزه به صورت گسترده ای در صنعت توزیع شده اند و از لحاظ جغرافیایی از سیستم های گردآوری داده های متمرکز جدا شده هستند .سیستم های اسکادا در یک سیستم کنترلی توزیع شده معمولا چندین سیستم تعاملی را کنترل می کنند که مسئولیت یک فرآیند محلی را بر عهده دارند.

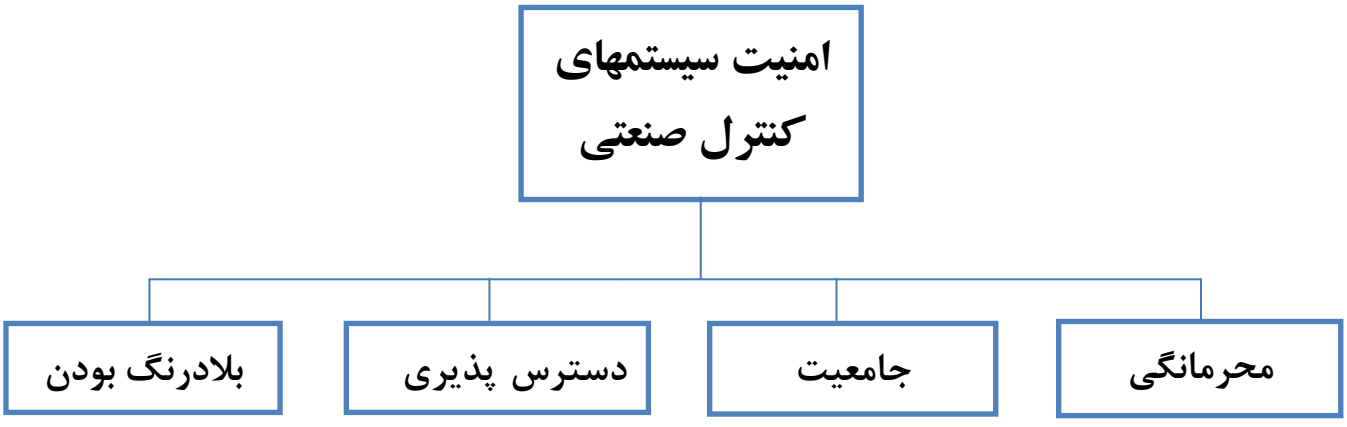
سیستم های کنترلی توزیع شده به صورت گسترده در صنایع مبتنی بر فرآیندهای فیزیکی استفاده می شوند .اما کنترل کننده برنامه پذیر منطقی یا یک سیستم نهفته مبتنی بر کامپیوتر است که می تواند تجهیزات صنعتی یا فرآیند

ها صنعتی را کنترل کند، همچنین توانایی مرتب کردن جریان اجرایی فرآیندها را هم دارد .سیستم های معمولا به همراه سیستم های اسکادا به منظور اجرا کردن عملیات های سرپرستی شده توسط اپراتور اسکادا مورد استفاده قرار می گیرند.

اولین سیستم های کنترل صنعتی در سال نمی توانستند به یک شبکه خارجی متصل شوند، اما با این حال توانایی متصل شدن به یک شبکه محلی با یک محیط کنترلی بسته به همراه پروتکل های اختصاصی را داشتند .اما سیستم های کنترل صنعتی امروزی کاملا از پشته پروتکل TCP/IP، اجرا شدن شدن بر روی سیستم عامل های بلادرنگ و متصل شدن به اینترنت جهانی پشتیبانی می کنند .به همین دلیل در آینده ما با مسائل امنیتی بسیاری برای سیستم های کنترل صنعتی رو به رو خواهیم شد .سیستم های کنترل صنعتی قسمت کلیدی زیرساخت های حیاتی هستند . به همین دلیل به وجود آمدن یک مسئله امنیتی برای سیستم های مستقیما می تواند بر روی سیستم های زیر ساخت تاثیر بگذارد.

تعریف امنیت سایبری از دیدگاه سیستمهای کنترل صنعتی

پیش از آنکه به بحث در مورد ضرورت و اهمیت تست نفوذ بپردازیم، می بایست با مفهوم واژه امنیت سایبری از دیدگاه سیستمهای کنترل صنعتی آشنا شویم. از آنجا که بحث امنیت سایبری سیستم های کنترل صنعتی با تعریف امنیت در حوزه فناوری اطلاعات (IT) مشابهت دارد، پیش از هر چیز ابتدا مفهوم امنیت سایبری (از این پس به اختصار آن را امنیت مینامیم)تعریف و بیان میگردد.امنیت از دیدگاه IT متشکل از سه بخش محرمانگی، جامعیت و دسترسپذیری میباشد که هر یک تعاریف و ویژگی های منحصر به فردی دارند محرمانگی به مفهوم عدم اجازه دسترسی افراد غیر مجاز به اطلاعات درونی سیستم میباشد. از آنجا که اطلاعات موجود در این سیستمها حیاتی و افشای آنها ممکن است صدمات بیشماری به ساختار و عملکرد این سیستمها وارد نماید، ضرورت برقراری این اصل نمود پیدا میکند.

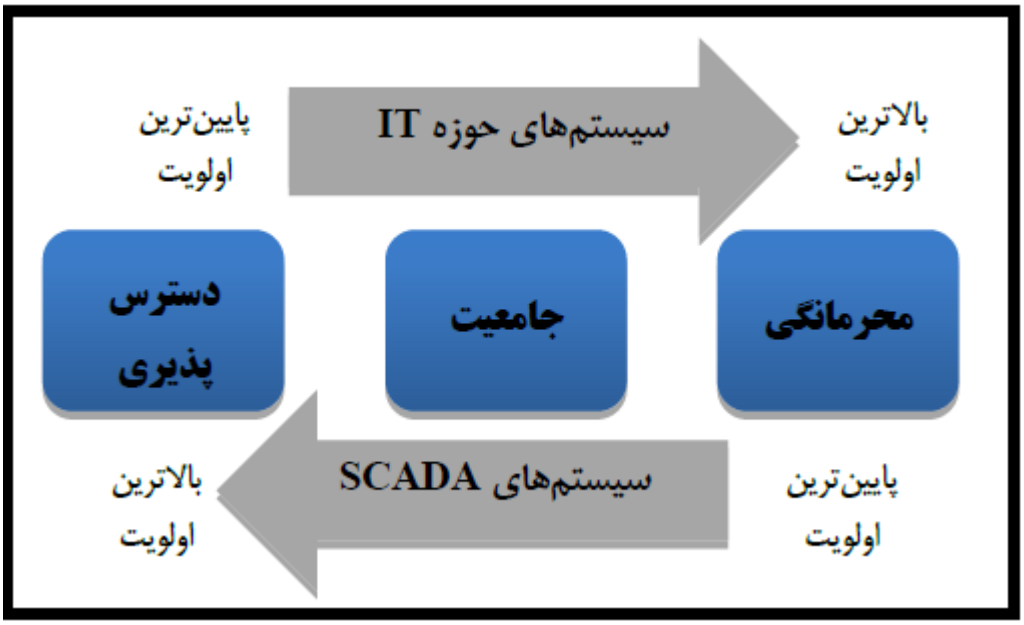


جامعیت بدین معناست که اطلاعات موجود در این سیستمها توسط افراد غیر مجاز قابل از بین رفتن و یا تغییر نباشند .منظور از افراد غیر مجاز کلیه افراد،پرسنل و یا هر گونه بدافزار و ویروسهایی میباشد که بدون اجازه دسترسی قصد اعمال تغییرات در سیستم را دارند .دسترس پذیری نیز به معنای قابلیت دسترسی افراد مجاز و مورد تایید به سیستم در هر زمان ممکن میباشد. برخورداری از این ویژگی در شرایطی که چندین کاربر غیر مجاز سعی در فراخوانی سیستم را دارند و در همان حال یک کاربر تایید شده نیز قصددسترسی به سیستم را دارد ضروری است .در این وضعیت سیستم میبایست این قابلیت را داشته باشد که بدون وقفه، درخواست دسترسی فرد مجاز را از بین چندین درخواست غیر مجاز تایید کرده و دسترسی را برای آن فرد مهیا نماید.

ویژگی دیگری که تنها در سیستمهای کنترل صنعتی(و نه فناوری اطلاعات)ضرورت دارد بحث بلادرنگ بودن دریافت و ارسال اطلاعات میباشدفرامین مربوط به سیستمهای کنترلی به ویژه واحدهای صنعتی مرتبط با زیرساختهای حیاتی میبایست به صورت آنی اعمال گردیده و گزارش دهی وتغییرات متناسب با آن صورت پذیرد در غیر اینصورت ممکن است خسارات مالی و جانی جبران ناپذیری برجای گذارند.

تفاوتهای امنیت حوزه فن آوری اطلاعات و سیستمهای کنترل صنعتی :

از آنجا که امروزه سیستمهای کنترل صنعتی همپوشانی وسیعی با سیستمهای حوزه IT دارند، تمامی آسیبهایی که تجهیزات حوزه فناوری اطلاعات را تهدید میکنند، تهدیدی برای سیستمهای کنترل صنعتی نیز محسوب میگردند .با این حال تفاوتهای بیشماری که بین این سیستمها وجود داردچالشهایی را در ایجاد امنیت سیستمهای کنترل صنعتی به وجود میآورند که باعث به وجود آمدن رویکردهای جدیدی در تعیین امنیت سیستمهای عملیاتیمیگردد .یکی از مهمترین این تفاوتها تخصیص اولویتها در تعریف امنیت میباشد .این بدان معناست که در سیستمهای کنترل صنعتی و بویژه SCADA اولویت در بحث ایمنی در ویژگی دسترس پذیری میباشد درحالیکه در سیستمهای حوزه IT این ویژگی از کمترین اولویت برخورداراست .این امر به لحاظ ارتباط سیستمهای کنترلی با زیر ساختهای صنعتی ازجمله صنایع آب، برق، نفت، گاز، پتروشیمی و نیروگاهی و همچنین الزام دسترسی بدون تاخیر افراد مجاز به این سیستمها میباشد.



یکی دیگر از تفاوتهای بارز میان این دو گروه سیستم، مدت زمان پاسخگویی به دستورات و فرامین میباشد.
همانطور که اشاره شد، با توجه به کاربری سیستمهای کنترل صنعتی در زیر ساختهای حیاتی و حساس، بروزهرگونه مشکل امنیتی، اختلال و تاخیر در زمان عملکرد غیر قابل قبول میباشد. لذا از نظر زمان عملکرد، سیستمهای کنترل صنعتی در گروه تجهیزات زمان واقعی سخت قرار دارند. تجهیزات زمان واقعی سخت به سیستمهایی اطلاق میگردد که دستورات ارسالی و دریافتی از سوی آنها در بالاترین. اولویت اجرا در پردازندههای اصلی قرار میگیرد این در حالی است که سیستمهای حوزه IT تجهیزات زمان واقعی نرم هستند.
دیگر تفاوتهای اصلی موجود در سیستمهای کنترل صنعتی با سیستمهای حوزه IT درجدول زیر آورده شده است.

سیستم های کنترل صنعتی	سیستم های حوزه IT
• اطلاعات از دست رفته بازیابی نمی‌شوند و این امر می‌تواند منجر به وقایع بسیار خطرناک شود.	• می‌توان اطلاعات از دست رفته را از طرق پشتیبان‌گیری بازیابی کرد.
• نیاز به پاسخ دهی بلادرنگ دارد و تاخیر در این سیستم‌ها قابل اصلاح نیست.	• نرخ انتقال داده‌ای بالایی نیاز است و تاخیر قابل اصلاح است.
• سیستم‌ها همیشه باید پشتیبان داشته باشند زیرا باز ایستادن سیستم‌ها از فعالیت می‌تواند خطرات جانی به همراه داشته باشد.	• انجام عملیات بازیابی اطلاعات و راه-اندازی دوباره سیستم معمولاً نتایج بحرانی و خطرناک ندارد.
• استفاده از ضد ویروس‌ها در این سیستم‌ها به دلیل الزام آن‌ها بر بلادرنگ بودن بسیار سخت است.	• نرم‌افزارهای ضدویروس به صورت گسترده‌ای در دسترس و قابل استفاده می‌باشند.
• آموزش‌ها و آگاهی‌های امنیتی در این زمینه محدود است.	• آموزش‌ها و ایجاد آگاهی در مورد امنیت این سیستم‌ها بالا است.
• بسیاری از پروتکل‌هایی که در سیستم‌های SCADA و زیرمجموعه‌های آن استفاده می‌شود از رمزنگاری برای ارسال داده‌ها استفاده نمی‌کنند.	• از رمزنگاری استفاده می‌شود.
• تست نفوذپذیری به صورت روتین انجام نمی‌شود و می‌بایست با دقت بسیار بالا صورت پذیرد.	• تست نفوذ پذیری به صورت روتین انجام می‌شود.
• پیاده سازی و به روز کردن وصله‌های امنیتی روی این سیستم‌ها باید با دقت بالا و معمولاً با حضور تامین کننده سیستم‌ها و فروشندگان مربوطه انجام شود.	• وصله‌های امنیتی به راحتی روی سیستم‌ها پیاده سازی و به روز می‌شوند.

لزوم امنیت سیستمهای کنترل صنعتی :

امنیت این سیستمهای کنترل صنعتی ، به چند دلیل بسیار مهم هستند .اصلی ترین این است که، نفوذکردن یا تخریب کردن یکی از این سیستم ها می تواند تاثیرات بسیاری بر روی محدوده های مختلفی از زندگی ما در جامعه بگذارد، بطوری که این تاثیرات می توانند موجب از دست رفتن جان انسان ها گردند.

به عنوان مثال، نفوذ کردن به یک شبکه توزیع وکنترل هوشمند الکتریکی و قطع برق و آغاز خاموشی، میتواند باعث خسارت دیدن تمامی مشتریانی گردد که از آن منبع برق دریافت می کنند .به هر حال ما باید صبر کنیم و ببینیم وضیعت امنیت سیستم های فعلی چه تاثیری بر روی سیستم های کنترل صنعتی آینده می گذارد. اما دو تهدید مجزا برای یک سیستم کنترل زیرساخت مدرن وجود دارد که آنها را در اینجا بررسی خواهیم کرد.

اولین نوع تهدید برای سیستم های زیرساخت، دسترسی به برنامه های کنترلی بدون احراز هویت است. مانند دسترسی گرفتن انسان به سیستم های زیرساخت کنترلی یا تغییر در فرآیند کنترل توسط نفوذ یک ویروس و دیگر تهدیدات که مبتنی بر نرم افزار است.

دومین نوع تهدید برای سیستم های زیر ساخت دسترسی گرفتن به بسته های شبکه ابزار میزبانی است. در بیشتر حالات، مکانیزم های امنیتی ابتدایی بوده و یا هیچ نوع مکانیزم امنیتی درپروتکل های سیستم های کنترل صنعتی وجود نداردبنا بر این هر کسی که بتواند بسته ای به دستگاه های کنترل صنعتی یا هر سخت افزار صنعتی ارسال کند با کمی تلاش می تواند کنترل این سیستمها را در دست گیرد.

آسیب پذیریهای رایج در سیستمهای کنترل صنعتی:

علیرغم پیشرفت های بسیار زیادی که درساختار و عملکرد سامانه های صنعتی وجود داشته،این سامانه ها از دیدگاه سایبری دارای ضعف های بسیاری هستند و همین امر باعث شده که سامانه های صنعتی مورد تهدید و حملات سایبری قرار بگیرند .آسیب پذیری های موجود در بخش های مختلف سامانه های صنعتی این امکان را برای مهاجمین سایبری فراهم ساخته تا به فکر حمله به زیرساخت های حیاتی کشور، آسیب رساندن و یا ایجاد اختلال در فرآیند کاری آن ها برآیند.از آن جا که بروز هرگونه نارسایی در بخش های مذکور ممکن است اثرات مخرب و جبران ناپذیری بر امنیت اقتصادی و توانمندی های دفاعی کشور برجای گذارد، از این رو اهمیت شناخت تهدیدات،آسیب پذیری ها و یافتن راهکارهای تدافعی و بهبود امنیت این سامانه ها بیش از پیش احساس می شود.به طور کلی آسیب پذیری های موجود درسامانه های کنترل صنعتی را می توان به دو دسته ی عمده تقسیم بندی نمود:

۱. آسیب پذیری های موجود در سامانه های صنعتی از دیدگاه فیزیکی
۲. آسیب پذیری های موجود در سامانه های صنعتی از دیدگاه سایبری

به طور کلی برقراری امنیت در بخش های مختلف یک واحد صنعتی در سالیان متمادی یکی از چالش های اساسی برنامه ریزان و بهر ه برداران سامانه های صنعتی بوده و به صورت گسترده ای تمام مسایل برنامه ریزی و بهره برداری سامانه های صنعتی را تحت تأثیر قرار داده است .در گذشته، این چالشها بیشتر ناشی از خسارات وارده در

اثر حوادث طبیعی و خرابی های فیزیکی تجهیزات صنعتی بوده است، اما حرکت به سمت هوشمندکردن سامانه های صنعتی که ورود گسترده ی سامانه های اطلاعاتی، ارتباطی و رایانه ای به سامانه های صنعتی را در بر داشته، چالش های امنیتی جدیدی را در حوزه ی سایبری برای این سامانه ها ایجاد کرده است .دلیل ایجاد این چالش های امنیتی جدید، وابستگی شدید سامانه های صنعتی به سامانه های اطلاعاتی و ارتباطی است که امنیت آن ها را به یکدیگر وابسته می کند.

امنیت سایبری عبارت است از حفاظت ازمالکیت معنوی با ارزش و اطلاعات کسب و کاربه صورت دیجیتال در برابر سرقت و سوء استفاده که به طور فزاینده ای به یک مسأله ی مهم مدیریتی تبدیل شده است .در حال حاضر بیش از هرزمان دیگری، حفاظت از فناوری های موجود درزیرساخت های حیاتی کشور در برابر آسیب های مخرب و استفاده ی نامناسب، نیازمند اعمال محدودیت های هوشمند بر چگونگی دسترسی کارکنان، مشتریان و شرکا به اطلاعات و برنامه های سازمان و واحدهای صنعتی می باشد .اکثر سازمان ها با قراردادن حفاظتی پیچیده در محیط اطراف خود سعی بر رسیدن به امنیت سازمان دارند .هرچند استفاده از این روش تا حدودی باعث بهبود و ارتقای امنیت فیزیکی سازمان می شود ولی مقوله ی امنیت سایبری چیزی فراتر از آن است که بخواهد با بکاربردن سامانه های حفاظتی در محیط اطراف سازمان به مرحله ی قابل قبولی برسد.

بخش های آسیب پذیر سامانه های صنعتی از دیدگاه سایبری:

به طور کلی سامانه های DCS و ،SCADA سامانه های کنترل صنعتی هستند که امروزه در صنعت از جایگاه ویژه ای برخوردار می باشند. دریک واحد صنعتی، سامانه ی کنترلی DCS متشکل از چندین PLC و تجهیزات فیلد از جمله حسگر،شیرها و غیره می باشد که این تجهیزات از طریق شبکه های صنعتی با هم در ارتباط می باشند.

SCADA نوع دیگری از سامانه های کنترل است که نسبت به DCS پا را فراتر گذاشته و در یک مقیاس بزرگ تر مورد استفاده قرار میگیرد. در واقع این سامانه نه تنها بخش های کنترل وارتباطات شبکه ای را در سطوح کنترل و فیلد پوشش می دهد، بلکه دارای قابلیت کنترل و پایش فرآیند صنعتی از راه دور به مسافت چند کیلومتر و حتی در بعضی موارد چندصد کیلومتر می باشد.کاربرد ای نگونه سامانه ها در صنعت بسیار زیاد است و می توان به مواردی از قبیل صنایع پتروشیمی،نفت، گاز، نیروگاه های برق و غیره اشاره کرد پس از آشنایی با ساختار و نحوه ی عملکردسامانه های کنترل صنعتی از جمله DCS وSCADA باید بخش های آسیب پذیر سامانه تفکیک و به طور جداگانه بررسی شوند.درواقع آسیب پذیری هایی که در سامانه های صنعتی وجود دارد متوجه چهار بخش اصلی است که در ادامه مورد بررسی قرار میگیرد.

۱)کنترل کننده های صنعتی PLC :

PLC به معنای کنتر لکننده ی منطقی برنامه پذیراست که از قسمت ورودی خود اطلاعات فرآیند را دریافت و آن ها را طبق برنامه ای که در حافظه اش ذخیره شده پردازش می نماید و نتیجه عملیات را از قسمت خروجی به صورت دستورها و فرامین کنترلی به گیرنده ها و اجراکننده های فرمان ارسال میکند .در گذشته با توجه به این که کنترل فرآینده ای صنعتی به عهده ی مدارهای فرمان رله ای بوده، آسیب پذیری و تهدیدات سایبری وجود نداشته

است ولی رفته رفته با ظهور PLCها در صنعت که خود یک مینی رایانه می باشند.آسیب پذیری هایی گزارش شده که استفاده ازاین آسیب پذیری ها می تواند منجر به حملات سایبری بسیار خطرناکی شود .همانطور که درسیستم عامل ها، نرم افزارها و سرویس های ارتباطی آسیب پذیری هایی وجود دارد، در PLC ها نیز اینگونه آسیب پذیری ها خود را نشان داده و همین امر باعث شده که این تجهیزات بسیار حیاتی به شدت مورد تهدید قرار بگیرند.

۲) پروتکل های ارتباطی مورد استفاده در صنعت:

پروتکل های ارتباطی در سامانه های صنعتی دارای مزایای بسیاری می باشند .به طور خلاصه مزایای مهم استفاده از پروتکل های صنعتی را می توان به صورت زیرشمرد.

- کاهش سیم کشی
- کاهش فضای اشغال شونده جهت نصب
- کنترل صحت اطلاعات و آشکارسازی خطا به دلیل استفاده از سیگنال دیجیتال به جای آنالوگ
- مصونیت بیشتر در مقابل نویز
- تست و عیب یابی راحت تر به دلیل وجود ساختار توزیع شده
- بازبودن سامانه و امکان استفاده از محصولات سازندگان مختلف روی یک شبکه

از پروتکل های معروف در زمینه شبکه های صنعتی می توان به موارد زیر اشاره کرد:

Profibus
Ethernet
AS-i
EtherCAT
Foundation Fieldbus
HART
Modbus
CANOpen
DNP 3

اهم آسیب پذیری های سایبری سامانه های کنترل صنعتی و پروتکل های مورد استفاده که ریشه درساختار و نوع طراحی آن ها دارد می توان به موارد زیر اشاره نمود:

- استفاده از سامانه های احراز هویت بسیارساده و نا امن
- عدم استفاده از روش های رمزنگاری اطلاعات
- عدم قابلیت رفع خطا در هنگام بروز مشکل در سامانه

۳) سیستم عامل و نرم افزارهای برنامه نویسی و پایش

PLC ها جهت کنترل فرآیند صنعتی باید توسط نرم افزارهای مهندسی مختص به خود، برنامه ریزی شوند. این نر م افزارها برای PLC شرکت های مختلف متفاوت می باشند و هر شرکت برای برنامه نویسی PLC های خود نرم افزارهایی را ارایه کرده است. به عنوان مثال شرکت زیمنس نرم افزاره ای مختلفی عرضه کرده که ابزار Step 7 یک نمونه از آن هاست. از طرفی جهت کنترل و پایش فرآیندهای صنعتی توسط کاربران، نرم افزارهای پایش عرضه شد که نرم افزارهای WinCC و Citect از آن جمله می باشند. سیستم عاملی که معمولاً برای کاربردهای مذکور استفاده می شود Windows بوده و دارای نسخه های مختلفی می باشد.

سیستم عامل و نرم افزارهای مورد استفاده در صنعت دارای آسیب پذیری هایی بوده که یک مهاجم می تواند با سوء استفاده از آن ها به سامانه کنترل نفوذ کرده و کنترل فرآیند را در دست بگیرد .در سال های اخیر آسیب پذیری هایی مربوط به سیستم عامل و نر م افزارهای مورد استفاده درصنعت از سوی مراکز امنیتی مختلف گزارش شده است که به عنوان مثال می توان به نرم افزار پایش WinCC اشاره کرد که توسط شرکت زیمنس تولید شده است .

٤) تجهیزات شبکه ای مانند مسیریاب ها و سوییچ ها

علاوه بر PLC ها و تجهیزات سطح فیلد،مسیریاب ها و سوییچ ها از جمله تجهیزاتی هستندکه در صنعت به وفور از آن ها استفاده می شود.اینگونه تجهیزات جهت پیاده سازی شبکه های صنعتی از اهمیت زیادی برخوردار می باشند.امنیت این تجهیزات بویژه هنگامیکه شبکه کنترل صنعتی به شبکه داخلی متصل می باشد بسیار حائز اهمیت می باشد.

هفت گام اساسی رایج جهت امنیت در سیستمهای کنترل صنعتی:

گام اول :ارزیابی سیستمهای موجود

یک سفر با علم به اینکه از کجا شروع می شود و به کجا ختم می گردد و روش طی مسیر چگونه می باشد ، برنامه ریزی می گردد.سفر به امنیت سیستمهای کنترل صنعتی با شناخت کامل از دارایی های موجود در شبکه و ارزیابی تهدیداتی را که شبکه را در معرض آسیب و خطر قرار می دهد (ارزیابی ریسک) آغاز می شود. با شناخت از دارایی های موجود در شبکه می توانیم مدیریت مناسبی را بر روی ریسک های احتمالی و کاهش آنها اعمال نماییم.در واقع خطر پذیری کاملا قابل حذف نمی باشد و حتی ممکن است بسیار هزینه بر باشد.بنابراین همیشه می بایستی درجه ای از رفع خطر پذیری قابل تصور باشد.یک مجموعه هیچگاه نباید سوال کند که ما چگونه می توانیم تمای خطرپذیری را حذف کنیم، بلکه واقع می بایستی به چگونگی کم کردن نسبی آن اهتمام ورزد.

برای پاسخ به این سوال مدیریت خطر پذیری مورد استفاده قرار میگیرد . مدیریت خطر پذیری یک دستیابی ساختیافته و سیستماتیک برای مدیریت پتانسیل هایی که توسط تهدیدات قابل از دست دادن می باشند. این تمهیدات توسط نفوذگران ، محیط و فاکتورهای دیگر ایجاد می شوند.

قدمهای مدیریت خطر پذیری:

مدیریت خطر پذیری در ۵ بخش تقسیم بندی میگردد:

۱. شناسایی اموال (موجودیتها)
۲. شناسایی تهدیدات
۳. بررسی نقاط آسیب پذیر

۴. ارزیابی خطر پذیری

۵. کاهش نمودن خطر پذیری

اولین قدم در مدیریت خطر پذیری تعیین اموال و موجودیتهایی می باشد که می بایستی حفاظت گردد. موجودیت به هر چیزی که ارزش مثبت اقتصادی داشته باشد می گویند و شناسایی موجودیتها فهرست بندی و مدیریت موجودیتها می باشد.

گام دوم :سیاستها ، رویه ها و دستورالعملها

پس از فهم مناسب از ارزیابی خطر پذیری در مجموعه و شناخت وضعیت موجود می توان به نگارش دستورالعملها و رویه ها پرداخت.بسیاری از شرکتها سیاستگذاری هاو دستورالعملهای بسیاری در حوزه فناوری اطلاعات اتخاذ نموده اند که می تواند پایه مفیدی برای سیستمهای کنترل صنعتی باشند ولی در سطح PLANT قابل تعمیم نمی باشند . به این دلیل تاکید می گردد که سیاستگذاری ها مختص سیستمهای کنترل صنعتی در نظر گرفته شود.اطلاع از قوانین امنیتی مختص هر سیستم یکی از عناصر ضروری جهت اتخاذ سیاستگذاری می باشد ولی به طور کلی در اینگونه سیستمها می بایستی موارد ذیل مد نظر قرار گرفته شود:

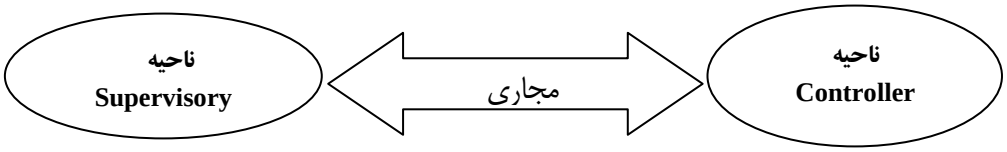
- دسترسی راه دور
- رساناهای قابل حمل
- مدیریت وصله ها
- مدیریت آنتی ویروس
- مدیریت تغییرات در سیستم
- پشتیبان گیری و باز نشانی
- نحوه پاسخ به رویدادها

گام سوم :آموزش اشخاص

هنگامیکه سیاستگذاریها ، دستورالعملها و رویه های امنیتی سازمانی شکل گرفت ، آگاهی کارکنان از وجود و اهمیت مسائل امنیتی حیاتی می باشد.بدین منظور می بایستی در ابتدا برنامه ای مدون جهت سازماندهی وضعیت آگاهی کارکنان توسط مسئولین بخش مربوطه به طور مستمر و مداوم انجام پذیرد و سپس برنامه آموزشی مختص وظایف هر شغل از قبیل مهندسین ، کارمندان اداری ، اپراتورها و کارکنان خدماتی صورت پذیرد.

گام چهارم :بخش بندی شبکه و سیستمهای کنترل صنعتی اشخاص

مهمتریت قدم تاکتیکی در ارتقا امنیت سیستمهای کنترل صنعتی ، قسمت بندی شبکه می باشد. قسمت بندی شبکه به مفهوم جداسازی اجزاء سیستم به منظور مجزا نمودن مناطق امنیتی و پیاده سازی لایه های حفاظتی برای ایزوله نمودن اجزاء حیاتی سیستمها می باشد.قسمتهای حساس شبکه می بایستی در ناحیه های مجزا تقسیم بندی گردند و سیاستهای امنیتی ویژه ایی اتخاذ گردد. ناحیه های امنیتی یکسان شامل اجزاء فیزیکی و یا منطقی می باشند که سیاستهای امنیتی مشابه ای برای آنان در نظر گرفته می شود.



هر ارتباطی ما بین نواحی می بایستی توسط مجاری خاصی تعریف گردد. مجاری دسترس پذیری به نواحی را کنترل و مدیریت می نماید و می تواند مانع حملاتی مثل حملات DOS گردد.

گام پنجم :کنترل دسترس پذیری به سیستم

هنگامیکه سیستم به چندین بخش مجزای امنیتی تقسیم گردید قدم بعدی کنترل دسترس پذیری به اجزای داخل هر زیر سیستم می باشد. کنترل می بایستی هم به صورت منطقی و هم به صورت فیزیکی مد نظر قرار گرفته شود.

کنترل فیزیکی شامل مواردی چون فنس ، درب های ضد سرقت ، کابینت های قفل دار و تجهیزات فیزیکی حفاظت می باشد. مفهوم کنترل فیزیکی در واقع محدود نمودن دسترسی به تجهیزات حساس و حیاتی شبکه می باشد به جز افرادی که می بایستی برای انجام دادن وظیفه خود وارد بخش گردند.

به طور مشابه کنترل منطقی نیز به همین شکل عمل می نماید. کنترل چند لایه احراز هویت جهت دسترسی به منابع سیستم ، کنترل دسترسی از راه دور افراد و به طور کلی تعیین اینکه چه افرادی با چه حقوقی به کدام سیستمها و در کدام زمان ها می بایستی متصل گردند ، در کنترل منطقی بررسی می گردد. تمامی افراد می بایستی بتوانند عملیاتی را انجام دهند که در حیطه وظایف کاری آنها باشد و گزارش عملیاتهای انجام شده هر فرد و وقایع صورت گرفته در سیستم ثبت شده و قابل دسترس باشد.

گام ششم :مقاوم سازی اجزای سیستم

مقاوم سازی اجزاء سیستم به معنای بستن و حذف توابع غیر قابل استفاده سیستمها به منظور جلوگیری از دسترسی غیر مجاز و یا تغییر می باشد. این مساله در سیستمهای کنترل مدرن بسیار دارای اهمیت می باشد. در سیستمهای کنترل صنعتی، غیرفعال نمودن توابع غیر قابل استفاده و اطمینان از تنظیمات صحیح مابقی توابع در بالاترین حد امنیتی آنها بسیار حیاتی می باشد. مسدود نمودن واسط های ارتباطی غیر ضروری و سرویسهای بلااستفاده روی این واسطها در تجهیزاتی مثل plc مهم می باشد. به عنوان مثال بسیاری از plc ها قابلیت اتصال از طریق وب را دارا می باشند ولی تا هنگامیکه نیاز مبرم به اتصال از این طریق وجود نداشته باشد می بایستی سرویس مد نظر غیر فعال گردد.هنگامیکه شبکه و سیستمها راه اندازی گردید می بایستی سایر اقدامات امنیتی از قبیل نصب آنتی ویروس و وصله های امنیتی انجام گیرد.

گام هفتم :نظارت و نگهداری سیستمها

به عنوان یک اپراتور و یا مالک سیستم کنترل صنعتی می بایستی به طور مداوم و هوشمند سیستم امنیتی خود را تحت نظر و مراقبت قرار دهید که این عمل شامل چندین فعالیت از قبیل به روز رسانی آنتی ویروس و نصب وصله های امنیتی و ... می باشد.

مرور رخدادهای سیستم و ثبت وقایع غیر معمول و بررسی آنها می بایستی مد نظر قرار گیرد.نهایتا تست دوره ایی تجهیزات و ارزیابی مداوم سیستم به منظور تشخیص تنظیمات صحیح امنیتی بر طبق آخرین استانداردهای موجود ، انجام پذیرد.

تست نفوذدر سیستمهای کنترل صنعتی:

در بحث ارزیابی آسیب پذیری، عملیات تست نفوذ یک گام فراتر از ارزیابی امنیتی قلمداد میشود .بسیاری از افراد، متخصصان، شرکت ها و سازمان هایی که در زمینه امنیت شبکه های سیستم های کنترل صنعتی فعالیت دارند به اشتباه این دو اصطلاح(تست نفوذ و ارزیابی امنیتی)را به جای یکدیگر به کار می برند .ارزیابی امنیتی فرآیندی است که در آن تمامی سرویس ها وسیستم ها برای مشکلات بالقوه امنیتی بازبینی می شوند و این در حالی است که در تست نفوذ عملاً بهره برداری از آسیب پذیری کشف شده صورت می گیرد و به شکلی واقعی به سیستم حمله می شود تا ثابت شود که سیستم دارای مشکل امنیتی است .در واقع تست نفوذ با شبیه سازی یک حمله واقعی و انجام نفوذ به سیستم، ارزیابی را فراتر از یک بررسی امنیتی خواهد برد.

لازم به ذکر است که از تست نفوذ حتی میتوان جهت ارزیابی در سطوح مدیریت پیکربندی تجهیزات و مدیریت شبکه جهت شناسایی آسیبهای بالقوه موجود نیز استفاده نمود .درواقع تست نفوذ را میتوان به عنوان یک تلاش مجاز و قانونی(هک قانونمند)برای نفوذ به شبکه های سیستمهای کنترل صنعتی و SCADA با هدف کشف آسیب پذیری و از بین بردن آنها

و در نهایت ایمن سازی شبکه های مورد نظر تعریف نمود .این فرآیند شامل جستجوی آسیب پذیری و نیز حمله به آن در جهت اثبات وجود آسیب پذیری میباشد .نتیجه یک آزمون نفوذ موفق مجموعه ای از پیشنهادهای مشخص برای آگاه سازی و رفع مشکلات امنیتی شناخته شده میباشد .

تست نفوذپذیری به دو صورت مختلف میتواند انجام گیرد:

جعبه سیاه :بدون دریافت هیچگونه دانش اولیه برای تست

جعبه سفید: دریافت کلیه اطلاعات زیر ساختی برای تست

معمولاً شرکتهایی که اقدام به انجام تست نفوذ مینمایند تنها خواستار یکی از موارد فوق میباشند .اما باید در نظر داشت که تست جعبه سیاه به لحاظ شبیه سازی حمله یک هکربسیار مفیدتر میباشد.

تست نفوذ، آسیبهای موجود در سیستمها و تجهیزات را شناسایی نموده و سندی مبتنی بر روشهای بهرهبرداری از این آسیبها که ممکن است توسط مهاجمین مورد استفاده قرار گیرند ارائه میدهد .در پروسه تست نفوذ روشهای مورد استفاده توسط مهاجمین جهت دسترسی غیر مجاز به سیستمهای کنترل صنعتی شبیهسازی شده و از آنها جهت کنترل تجهیزات استفاده میگردد .لازم به ذکر است که تست نفوذ در سیستمهای کنترل صنعتی میبایست به گونهای متناسب با تجهیزات و ساختار به کار رفته درهر واحد صنعتی صورت پذیرد .در اغلب موارد پیاده سازی گامهای آزمون نفوذ در شبکه های سیستمهای کنترل صنعتی با آنچه در حوزه فناوری اطلاعات انجام میپذیرد یکسان است . هر چند که روش و نحوه پیاده سازی تست نفوذ در این شبکه ها میبایست به شدت و با دقت بسیار بالایی کنترل گردد تا منجر به آسیب رساندن به بخشهای حساس زیر ساختهای حیاتی نگردد .در این میان تعامل میان متخصصین ارزیاب و کارشناسان سیستمهای کنترل صنعتی از اهمیت بالایی برخوردار است .تمامی مراحل انجام تست نفوذ، متدولوژیهای بکار رفته و اقدامات صورت گرفته، الزاماً باید با مهندسینسیستمهای کنترل صنعتی سازمان هدف در میان گذاشته شود .تمامی آزمونهایی که ممکن است به تجهیزات حیاتی آسیب برسانند میبایست حذف گردند .به طور کلی حفظ صحت و سلامت سیستمهای کنترل صنعتی در حین انجام فرایند تست نفوذ باید به درستی و با دقت بالایی رعایت گردد

مراحل اصلی فرایند تست نفوذ:

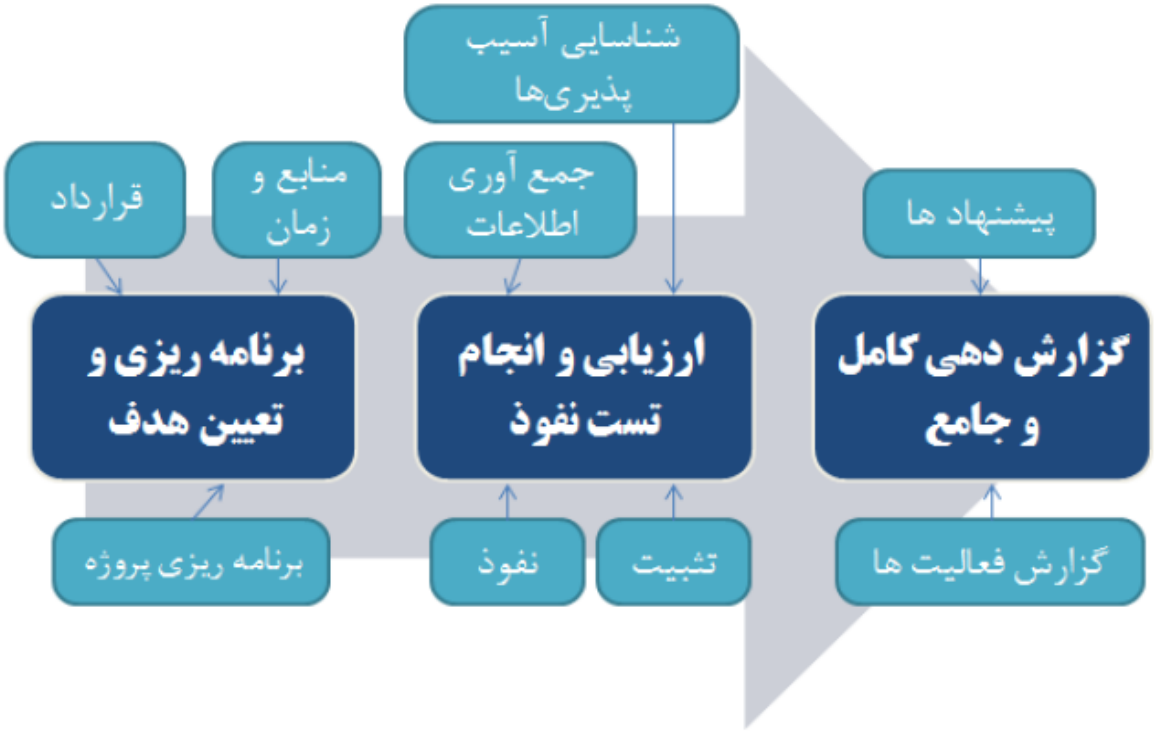
استانداردهای مختلفی در زمینه تست نفوذ سیستمهای حوزهی IT در دسترس بوده که قابل استفاده میباشند .برخی از این استانداردها مانند OWASPتنها به بحث نفوذ از دید برنامههای کاربردی تحت وب پرداخته اند درحالیکه گروهی دیگر همچون استاندارد ISSAF آزمون نفوذ را از دیدگاه شبکه مورد ارزیابی قرار میدهند .استانداردهای دیگری نیز دراختیار میباشند که به پیادهسازی تست نفوذ در هر دو قسمت پرداخته اند که از این میان میتوان به استاندارد PTES اشاره نمود .در این مقاله برآنیم تا به معرفی فرایند انجام تست نفوذ در سیستمهای کنترل صنعتی و SCADAبا در نظر گرفتن استانداردهای مطرح ارزیابی و آزمون نفوذ مورد استفاده در سیستمهای حوزه فناوری

اطلاعات و استانداردهای حوزه بپردازیم، سیستمهای کنترل صنعتی به طور کلی فرآیند انجام و پیاده سازی تست نفوذ در سیستمهای کنترل صنعتی در سه فاز به صورت زیر تقسیم بندی شده است:

فاز اول :طراحی و آماده سازی(برنامه ریزی و تعیین هدف)

فاز دوم :ارزیابی و انجام تست نفوذ

فاز سوم :گزارش دهی کامل و جامع



مراحل فرایند تست نفوذ

فاز اول طراحی و آماده سازی(برنامه ریزی و تعیین هدف):

اولین بخش از فرایند آزمون نفوذ، فاز طراحی و آماده سازی است که شامل تهیه طرح و اهداف کلی انجام تست نفوذ میباشد. اینکه چرا، چگونه و با چه مجوزهایی این اقدام صورت میپذیرد از اولویتهای کار بوده و میبایست پیش از هر اقدام دیگری مد نظر قرار گیرد. در این مرحله از فرایند تست نفوذ میبایست یک توافقنامه رسمی بین گروه ارزیاب و مسئولین صاحب نظرسازمان هدف، جهت دسترسی قانونی به تمامی قسمتها و شبکه های داخلی سازمان

صورت پذیرد. این طرح میبایست در برگیرنده اطلاعات کلی طرح اعم از تعداد و اعضای گروه ارزیابی، تاریخ و زمان دقیق شروع ارزیابی، نحوه وچگونگی پیادهسازی آن و دیگر اطلاعات ضروری جهت انجام تست نفوذ باشد.

فاز دوم ارزیابی و انجام تست نفوذ:

این فاز در واقع به عنوان فاز اصلی تست نفوذ تلقی میگردد .این مرحله که طی یک روند گام به گام انجام میگردد، در برگیرنده تمامی قسمتهای عملیاتی و حوزه فنی انجام تست نفوذ باشد .این مراحل شامل بخشهای زیراست:

۱. جمع آوری اطلاعات
۲. شناسایی آسیب پذیریها
۳. نفوذ و بهره برداری از آسیب پذیریها
۴. تثبیت دسترسی به سیستم و از بین بردن ردپاها

اعمال و پیاده سازی مراحل فوق از الزامات انجام کامل و جامع تست نفوذ بوده و میبایست به همان صورت گام به گام فوق انجام پذیرد تا نتایج مطلوب و موثری در بر داشته باشد .تمامی مراحل فوق به صورت مجزا در زیر تشریح شده اند.

۱)جمع آوری اطلاعات:

جمع آوری اطلاعات اولین و مهمترین قدم در انجام تست نفوذ میباشد. در این مرحله سعی میشود تمامی اطلاعات مربوط به سیستمهای کنترل صنعتی سازمان هدف، نوع سیستم عامل، مدل و نوع تجهیزات صنعتی و به طور کلی تمام اطلاعات مورد نظر، از روشها و راههای مختلف جمع آوری شود.

وابستگی شدید فازها و مراحل بعدی به این مرحله، اهمیت این مرحله را برجسته تر مینماید. بعد از انجام این فاز گروه ارزیاب میبایست نقشهای ازشبکه های سیستمهای کنترلی موجود به همراه جزئیات کامل و همچنین اطلاعات مربوط به سیستم هدف را بدست آورده باشند. به علاوه شناسایی نوع سیستمهای فعال در شبکه جهت انجام تست نفوذ بسیار حائز اهمیت میباشد(نوع سیستم عامل و اطلاعات مربوط به آنها) این امر در انتخاب ابزارها وتکنیکهای مناسب جهت نفوذ بسیار مهم تلقی میگرددجمع آوری اطلاعات به طور کلی به دو نوع تقسیم بندی میشود .نوع اول نوع غیر فعال است که در آن، هدف کسب اطلاعات هرچه بیشتر از سیستمها و یا شبکه مورد ارزیابی است، بدون آنکه ارتباط مستقیمی با آن شبکه ایجادگردد .در این نوع از جمع آوری اطلاعات، تنها داده هایی از شرکت و سازمان(مالکیت سازمان، آدرس شرکت یا سازمان، محل قرار گیری شبکه و سیستمهای سازمان، اطلاعات مربوط به نقشه فیزیکی، شماره تماس، پست الکترونیک و درجه و رتبه کارکنان) مورد توجه هستند که با اهداف پروژه

تست نفوذ مرتبط باشند.نوع دوم را جمع آوری فعال مینامند که در آن با سیستمهای هدف مورد نظر، ارتباط مستقیم برقرار میشود .این نوع جمع آوری اطلاعات درک بهتر و بیشتری از دامنه فعالیتها، ویژگیها و نوع سیستمهایی که در پروژه هستند در اختیار کارشناسان ارزیابی و آزمون نفوذ قرار میدهد .نمونه بارزی از این نوع جمع آوری اطلاعات را میتوان در بدافزار Stuxnet مشاهده نمود.این بدافزار برای مدت طولانی در سیستمهای کنترل صنعتی و تاسیسات هستهای ایران در حال جمع آوری اطلاعات جهت ضربه زدن به آنها بود طی این مدت مهاجمین سازنده این بدافزار توانستند اطلاعات جامع و دقیقی از تاسیسات هسته ای مورد نظر خود بدست آورده و با محدود کردن نوع فعالیت و ارتقاء بدافزار خود، به طور دقیق به هدفهای مورد نظر آسیب رسانند .به طوری که طبق گزارشات حاصله، بیشترین آسیب را از بین تمامی سیستمهای کنترل صنعتی مورد استفاده در سرتاسر دنیا، تنها بر یک نوع ومدل خاص از PLC های مورد استفاده در ایران که وظیفه مشخصی داشتند وارد آوردند.

۲)شناسایی آسیب پذیریها:

شناسایی آسیب پذیریها در قدم بعدی جمع آوری اطلاعات قرار میگیرد .درواقع در این مرحله با استفاده از اطلاعات بدست آمده در مرحله قبلی سعی در بدست آوردن فهرستی از سیستمهای آسیب پذیر موجود در شبکه سیستم هدف میگردد .در این مرحله ابزارهایی به عنوان پویشگر آسیب پذیری مورد استفاده قرار میگیرند که از آن جمله میتوان به Nessus ،Corimpact اشاره نمود .هرچند ابزار Nessus از Pluginهای مختص ارزیابی سیستمهای SCADAبهرهمند میباشد اما توصیه میشود پیش از استفاده از آن، تغییرات لازم متناسب با نوع ارتباطات شبکه ها و تجهیزات صنعتی مورد استفاده در سازمان هدف اعمال گردد .این امر از آن جهت اهمیت دارد که بروز هرگونه اختلال در فرایند کاری تجهیزات صنعتی، ممکن است موجب توقف یک پروسه و در پی آن بروز حوادث جانی و مالی بیشماری گردد.این مرحله با استفاده از اطلاعات بدست آمده از گام قبلی، به شناسایی آسیبپذیریهای موجود در سیستم میپردازد .در واقع در این مرحله راههای نفوذ به شبکه مورد نظر به عنوان مسیرهای بالقوه آسیبپذیری شبکه معرفی میگردند تا در صورت نیازمندی به آنها در مراحل بعدی آزمون نفوذ مورد استفاده قرار گیرند از جمله آسیبپذیریهای رایج در سیستمهای کنترل صنعتی میتوان به ضعف یا عدم رمزنگاری اطلاعات احراز هویتی کاربران در هنگام ارسال ودریافت اطلاعات اشاره نمود .بهره برداری از این آسیبپذیری، این امکان را برای مهاجمین فراهم مینماید تا از طریق بازیابی و بررسی اطلاعات انتقالی بین شبکهای، بدون ارسال حتی یک بسته اطلاعاتی، به سیستم میزبان دسترسی کامل یابند .پویشگرهای آسیبپذیری مذکور امکان شناخت وکشف آسیب فوق را جهت شناسایی و رفع، در اختیار تیم ارزیابی قرار میدهند.

۳)نفوذ و بهره برداری از آسیبپذیریها

روشها و متدهای پیشرفته بسیاری برای انجام نفوذ به سیستمهای کنترل صنعتی وجود دارد .دسترسی به این روش ها به علت وجود ضعفهای امنیتی بیشمار موجود در تجهیزات سیستمهای کنترل صنعتی بوده که هر روز بر تعداد این نواقص و در پی آن راههای دسترسی ونفوذ به تجهیزات مختلف کنترلی افزوده میشود .از آنجایکه بستر های ارتباطی سیستمهای مدرن SCADA عموماً با اینترنت، شبکه سوئیچینگ مخابرات، شبکه های ماهوارهای، شبکه های بیسیم و شبکه های واحد های اداری سازمانها در ارتباط است، راههای بالقوه مختلفی جهت نفوذ به این سیستمها وجود دارد .به طور کلی نفوذ به سیستمهای SCADA میتواند ازطریق یکی از بسترهای ارتباطی زیر صورت گیرد:

- ارتباط اینترنتی
- شبکه های ارتباطی اداری و بین سازمانی
- ارتباط با شبکه هایی که دارای آسیبپذیری هستند
- ارتباط ناامن در بسترهای ارتباطی بیسیم
- از طریق آسیب پذیری در پروتکلهای ساده مدیریت شبکه که جهت جمع آوری اطلاعات و اطلاع رسانی از رویدادهای شبکه مورد استفاده قرار میگیرد.
- پورت های باز رایانه ای
- تراکنشهای پست الکترونیکی در شبکه های کنترلی
- خطوط شخصی استیجاری
- حملات به وسیله کرمها و ویروسها
- حملات درون سازمانی مانند کارمندان ناراضی، استفاده غیر مجاز از نرم افزارهای نامناسب، تغیر در پیکربندی سیستم توسط کارمند بدون مجوز

۴) تثبیت دسترسی به سیستم و از بین بردن ردپاها:

پس از دسترسی و نفوذ به سیستم هدف، میبایست اقداماتی جهت حفظ این دسترسی به نحوی که اثری از نفوذ برجای نماند صورت گیرد. در این راستا رعایت نکات زیر الزامیست.

- تمامی ابزارها و کدهای بهره برداری مورد استفاده چه در زمان انجام تست و چه پس از آن میبایست پنهان سازی گردند.
- ثبت کننده های فعالیت کاربران و نتایج حاصله میبایست پنهان سازی گردند.
- تمامی فعالیتهای بدون مجوزی که گروه ارزیاب از سوی سیستم هدف به سمت شبکه های دیگر صورت میدهند میبایست از کانالهای پنهان انجام پذیرد.

رعایت نکات ذکر شده بسیار ضروری و از الزامات انجام تست نفوذ تلقی میگردد .اهمیت این امر از آنجا است که در صورت انجام آشکارای تست نفوذ، ابزارهای امنیتی نصب شده بر روی شبکه سیستم هدف همانند Firewallها و Antivirus ها کاربران را از ورود به سیستم مطلع ساخته وکاربران میتوانند با تغییر شرایط امنیتی، آسیبپذیری کشف شده را پیش ازاعلام گزارش نهایی برطرف نمایند.

جهت برطرف نمودن ردپاها و پنهان سازی ابزارهای نفوذ میتوان از تکنیکهای زیر استفاده نمود:

- تغییر نام پوشه ها با اسامی مشابه آنچه در سیستم هدف وجود دارد.
- قرار دادن فایلها در چندین پوشه تو در تو
- قرار دادن فایلها در پوشه های غیر قابل دسترسی

فاز سوم :گزارش دهی کامل و جامع

در پایان فرایند تست نفوذ میبایست یک گزارش نهایی حاوی تمامی اطلاعات گردآوری شده در حین انجام آزمون، نتایج حاصله، روشها و توصیه هایی جهت رفع آسیب پذیریهای کشف شده آماده و به صاحبان صنایع تحویل گردد. در این راستا ارائه بخشهای زیر در گزارش نهایی الزامی است:

- خلاصه اجرایی
- محدوده انجام آزمون نفوذ
- ابزارهای مورد استفاده
- تاریخ و زمان دقیق انجام تست
- گزارش تمامی نتایج حاصله از انجام تست
- لیست تمام آسیب پذیریهای کشف شده به همراه توصیه های لازم جهت رفع آسیب پذیری

پس از ارائه گزارش نهایی، تمامی فایلهای ایجاد شده در سیستم هدف می بایست حذف گردند. درصورتیکه این امر امکان پذیر نباشد میبایست لیست تمامی فایلها و محل قرارگیری آنها در سیستم هدف ذکر گردد تا متصدیان داخلی سازمان قادر به برطرف نمودن و حذف آنها باشند.