بسم الله الرحمن الرحیم

نام پروژه:

آسیب شناسی شبکه رایانه ای، سامانه ها و ارتباطات، طراحی امنیت ، نظارت و واکنش سریع در

شبکه رایانه ای دانشگاه امام صادق (ع)

تاریخ تهیه پیشنهاد:۲۰ آبان ماه ۱۳۹۷

تهیه کننده: تیم مهندسی فروش شرکت ایمن رایانه پندار

الزامات وحداقل نیازهای بخش فناوری اطلاعات

- Sniff کردن ترافیک شبکه و بررسی ضعف های موجود شبکه
- انجام تست نفوذ پذیری بر روی سرور ها، کلاینتها، روترها، پروکسیها، نرم افزار های تحت وب، فایروالها، ابزارهای کنترل دسترسی، مودمها و... برای اطلاع از پورت ها و حفره های باز و تشخیص و شناسایی سرویس های آسیب پذیر
- کشف username/password ها از طریق حملات dictionary attack و Brute force بر روی سیستم ها
- شناسایی جزئیات سرویس های موجود (Service fingerprinting)
- اطلاع از تعداد انواع ریسک تخریبی و محل اختفای کدهای مخرب و نیز از کلیه حفره ها و نقص های امنیتی موجود در شبکه
- تخمین اثرات آسیب های شناسایی شده و دسته بندی آنها
- تهیه گزارش آسیب پذیری های شناسایی شده
- ارائه آخرین تکنولوژی روز شبکه در راستای برقراری امنیت شبکه
- تامین نیازهای مرتبط با امنیت شبکه
- کنترل، مدیریت و بهینه سازی پهنای باند جهت استفاده از برنامه های کاربردی
- ابزارهایی برای نظارت شبکه
- مدیریت نحوه استفاده کاربران از اینترنت.
- مانیتورینگ ترافیک شبکه
- ارائه راهکاری جهت محافظت از اطلاعات سازمان در برابر حوادث و دسترسی های غیر مجاز از داخل و خارج سازمان
- تست و بهینه سازی سطح دسترسی های کاربران
- مدیریت وپیکره بندی تجهیزات
- ارائه نرم افزاری جهت ارزیابی خودکار شرایط امنیتی در شبکه داخلی
- امن سازی مسیرهای عبور دیتا
- پیاده سازی سیستم جهت کنترل پورت USB

مراحل انجام کار:

- انجام تستهای نفوذ در شبکه داخلی، وب سایت و ارتباطات درون / برون شبکه ای، بمنظور آسیب شناسی. برای انجام این مهم، میبایست متدولوژی تست نفوذ بصورت مستند بیان گردد. تلفیقی از مهارتهای فردی و ابزارهای کارامد مورد استفاده قرار گیرد. ابزار های بکار گرفته شده در این قسمت میبایست قابل اطمینان و کارامد بوده و خروجی های آن بر مبنای استاندارد های امنیت اطلاعات ISO 27001 تنظیم گردد. کارشناسان نفوذگر نیز میبایست معرفی گردند تا علاوه بر بعد فنی، از لحاظ سوابق کیفری و... نیز در صورت نیاز به تائید دانشگاه برسند.

کارشناسان نفوذگر می بایست پس از تست های اولیه نتایج ارزیابی خود را در قالب گزارش" ارزیابی اولیه" به واحد فناوری اطلاعات سازمان ارائه نمایند، تا پس از تائید این واحد اقدام به برطرف نمودن آسیب پذیری ها و حفره ها بنمایند.

پس از این مرحله می بایست شرکت، سامانه ای جهت ارزیابی خودکار وضعیت فعلی امنیت شبکه ارائه نماید که قادر باشد با موتور ضد ویروسی غیر از Kaspersky کدهای مخرب و تهدیدهایی را که به هر نحو از لایه های امنیتی شبکه عبور کرده و به درون محیط سازمانی رسیده اند را کشف و پاکسازی کند. لازم بذکر است سامانه معرفی شده نباید بهیچ عنوان با ضد ویروس ها و فایروالهای دیگر ناسازگاری داشته باشد. این سامانه می بایست دارای False Positive پائین باشد و در پایان هر بار پویش شبکه، گزارش جزء به جزء کدهای مخرب شناسایی شده را به تفکیک هر سیستم با IP و یا Computer Name ارائه دهد.

- پس از برطرف نمودن کلیه کدهای مخرب، حملات و تهدیدات، حال نوبت به نگهداشت این وضعیت است. ارائه ابزار های مناسب جهت حفظ وضعیت امن کنونی راهگشای این مشکل است.با عنایت به نیاز سازمان به کنترل ترافیک شبکه و کنترل کاربران در خصوص سطح دسترسی ها و سایر نیاز های مطروحه در فوق، می بایست ابزار های مناسب و جامعی ارائه گردد. شایان ذکر است امکان کنترل واحد و متمرکز این اقدامات از طریق ابزار های معرفی شده از امتیاز بالایی برخوردار است.

۱. حوزه کاری (Scope of Work)

بطورکلی حوزه عمل آزمون های امنیتی شامل موارد زیرخواهد بود:

- سرورهای که مورد استفاده مشتریان هستند ، سرورهای عمومی (Extranetها، سرویسهای تحت اینترنت، VPN) ،ابزارهای Internetworking (روترها و...) ، اجزای ساختارهای امنیتی (فایروالها،پروکسی ها،ابزارهای کنترل دسترسی) و ابزارهای remote-access (ترمینال سرورها، مودمهاو.....) و ایستگاههای کاری برای استفاده های روزمره
- مکانیسم و تدابیر امنیتی برای عرضه کنندگان فن آوری، بسترهای ارتباطی یا سرویسهایی که مستقیما با ساختار IT مجموعه در ارتباط هستند.

۱-۱. نحوه انجام تست:

برای هرکدام از آزمونها، حملاتی که پوشش دهنده دامنه های مختلف باشند، برنامه ریزی خواهد شد. مراحل زیر این تقسیم بندی را مشخص می کند:

۱-۱-۱. مرحله اول - حمله بیرونی

برای بررسی حمله یک نفوذگر بیرونی که تنها اطلاعات عمومی قابل دسترس از هدف در اختیار دارد،تیم مجری آزمون اقدام به نفوذ به مکانیسم های امنیتی در سطح شبکه و نیز مکانیسم های کنترل دسترسی به سرورها خواهد نمود.حملات غیر فعال (Passive) برای جمع آوری اطلاعات از اینترنت ، مستندات منتشر شده روی وب سایتها وغیره در کنار حمله فعال (Active) به این مکانیسم ها با تمرکز روی مشکلات مربوط به طراحی،نصب و تنظیم سیستم عامل و نرم افزار پایه، انجام خواهد شد.

دسته بندی آزمون ممکن است شامل اقدامات زیر باشد(نه لزوماً محدود به این موارد):

- ✓ اجرای آزمونهایی برای جمع آوری اطلاعات: اقدام برای شناسایی میزبانها، توپولوژی شبکه، سیستم های عامل، سرویسهای ارائه شده، مکانیسم های کنترل دسترسی،Access Server ها و ارتباط بین سیستم‌ها
- ✓ آزمونهای ضعفهای امنیتی عمومی: اقدام برای شناسایی ضعفهای شناخته شده و مشهور و بهره گیری از آنها برای نفوذ که شامل ضعفهای امنیتی مربوط به سرویسهای سیستم عامل مانندIMAP/POP,DNS,SMTP,FTP,HTTP و غیره می شود.
- ✓ آزمونهای مرتبط با خصوصیات و توپولوژی شبکه: اقدام برای شناسایی ضعفهای مرتبط با توپولوژی شبکه و نفوذ از طریق آنها،ضعفهای مرتبط با تنظیمات اجزا،اصول طراحی و پروتکل استفاده شده در شبکه که شامل آزمونهایی مانند تکنیکهای Spoofing و آزمونهای مختص پروتکل(مانند تست fragmentation IP options) ،خطاها در طراحی و پیاده سازی پروتکلهای مختلف شبکه و سرویسهای مربوط و غیره.
- ✓ آزمونهای مرتبط با نفوذ پذیری حاصل از تنظیمات: اقدام برای شناسایی و نفوذ از طریق تنظیمات ضعیف یا اشتباه متداول
- ✓ بررسی وجود backdoor ها: اقدامات برای شناسایی و نفوذ از طریق backdoor های شناخته شده که احتمالا در ساختار شبکه مورد ارزیابی،موجود باشند.
- ✓ آزمونهای مربوط به روشهای احراز هویت(Authentication) و کنترل دسترسی(Access Control) اقدامات برای نفوذ به مکانیسم های احراز هویت و کنترل دسترسی بر اساس روشهای معمول که از فقدان سیاست امنیتی قوی یا عدم اجرای آن استفاده می کنند،شامل حملات brute-force و Dictionary روی کلمات عبور و نفوذ به روشهای احراز هویت ضعیف

۲-۱-۱. مرحله دوم - حمله داخلی

پس از موفقیت در مرحله حمله خارجی و با استفاده از دسترسی ها و امکانات بدست آمده از این مرحله ، تعدادی آزمون امنیتی برای نفوذ امنیتی به سایت شبکه ای از داخل خود مجموعه انجام خواهد شد.این آزمونها بدون دریافت اطلاعات اضافی در مورد شناسه های کاربری یا نرم افزار های لازم برای کار با شبکه داخلی انجام خواهد شد.

حملات داخلی برای رسیدن به اهداف زیر انجام می شوند:

- بدست آوردن دسترسی مدیر سیستم(root/administrator/SYSTM و مانند آن) در سیستم های مورد نظر نفوذ قرار گرفته.
- دست آوردن دسترسی کاربرن خاص که بتوانند اطلاعات مورد پردازش سیستم را دستکاری کنند.(کاربر DBA , Webmaster و مانند آن).
- کسب امکان **خواندن** داده ها و اطلاعات محافظت شده و ارزشمند
- کسب امکان **مشاهده و تغییر** داده ها و و اطلاعات محافظت شده و ارزشمند
- کسب امکان دستکاری داده ها با بکارگیری سایر پروسس ها یا کاربران که لزوما به معنای کسب دسترسی آنها نیست.
- کسب امکان انجام عملیاتی مانند حذف محدودیتهای دسترسی یا مکانیسم مراقبتی(Audit) سیستم ها یا کاربران.

۲-۱. معیار های موفقیت

- اجرای موفق با نتایج مثبت: یک آزمون با نتایج مثبت در شرایطی مورد قبول خواهد بود که مجری آزمون به نحوی بتواند از اجزای سیستم امنیت اطلاعات سازمان یا اطلاعات پردازش شده توسط آن استفاده کند که در شرایط مشابه سودی را متوجه نفوذگر احتمالی نماید یا باعث هر نوع آسیب و ضرربه سازمان گردد.

- اجرای موفق با نتایج منفی: یک آزمون با ننتایج منفی در شرایطی مورد قبول خواهد بودکه تعداد قابل قبول اقدام برای نفوذ با ارائه گزارش آنها در زمان تعیین شده در قرارداد، توسط مجری آزمون انجام شده باشد یا اینکه یک روش حمله یا نفوذ معرفی شود که احتمال زیادی برای موفقیت آن وجود دارد، اما احتیاج به زمان یا منابع بیشتری از آنچه در قرارداد فعلی ذکر شده، دارد.

۳-۱. خروجی و نتایج آزمون

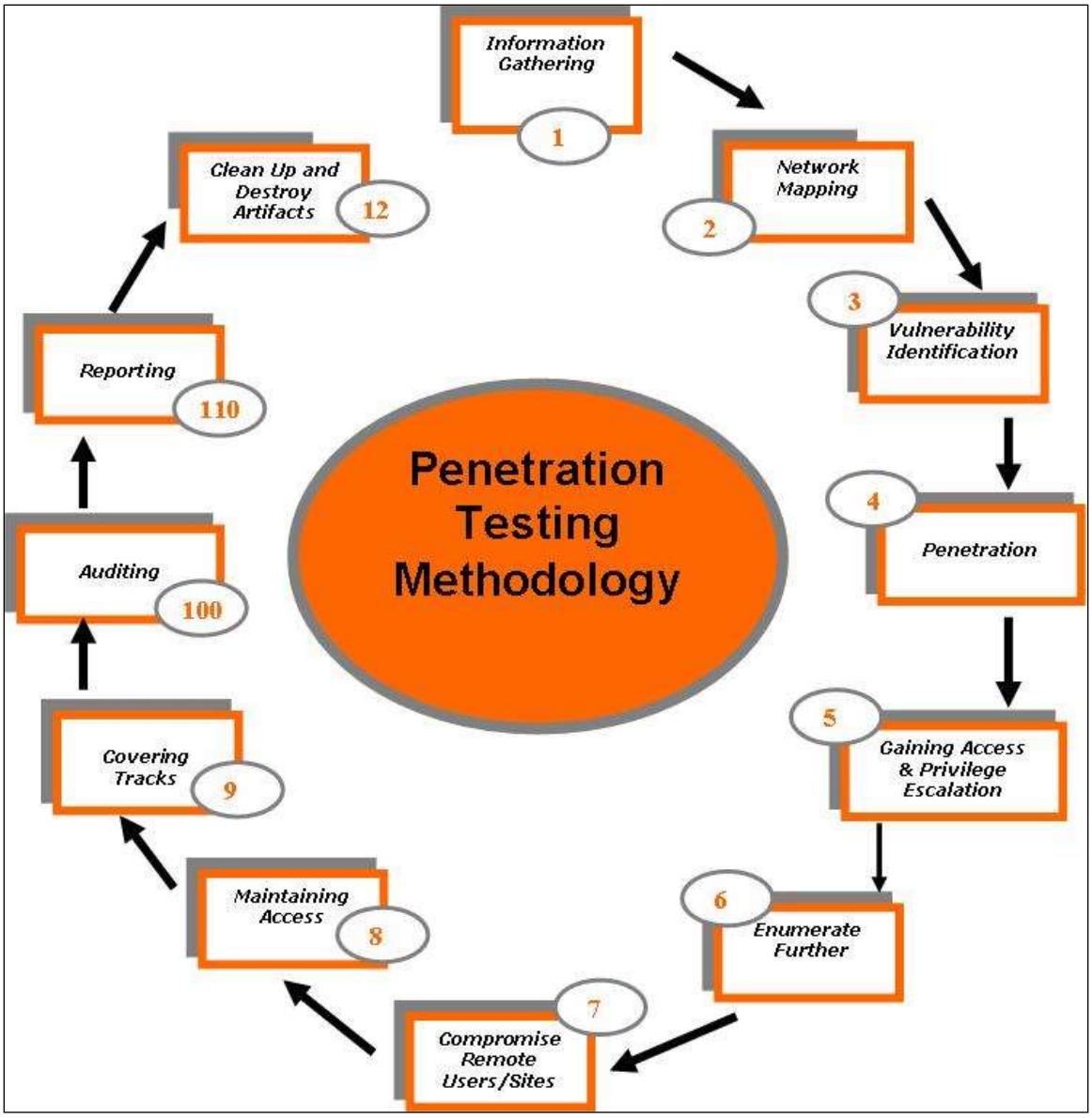
پس از پایان بررسی امنیتی و تست نفوذ پذیری , کارفرما در قالب گزارش هایی که از سوی شرکت ارائه گردیده , از مشکلات امنیتی , روش های نفوذ و خطراتی که این مشکلات امنیتی برای شبکه و سیستم ایجاد میکنند آگاهی خواهد یافت . همچنین در خلال گزارش های ارائه شده از سوی شرکت , راهکارهای کلی برای مقابله با این نقاط ضعف ارائه خواهد شد . شرکت در قالب بررسی امنیتی و تست نفوذ پذیری , هیچگونه مسئولیتی در قبال ارائه راهکار جامع امنیتی برای مشکلات شناسایی شده , و یا رفع مشکلات شناسایی شده نخواهد داشت .

۲. متدولوژی آزمون نفوذ پذیری

تست نفوذ پذیری (Penetration Test) یکی از مراحل مهم یک ممیزی امنیتی (Security Audit) میباشد . با استفاده از نتایج تست های نفوذ پذیری , سازمان مورد بررسی قادر خواهد بود تا با شناخت و آگاهی کاملی که نسبت به نقاط ضعف زنجیره امنیتی , تهدیداتی که متوجه سیستم میباشند و تخمین ریسک های حاصل از هریک از این موارد که از طریق بررسی امنیتی بدست آمده , اقدام به طراحی راهکار امنیتی جامع و کارآود برای سازمان و مجموعه خود نماید . بر این اساس طراحی و اجرای راهکارهای امنیتی سازمان , برای دستیابی به سطح امنیتی قابل قبول با دیدی بهتر و دقت بیشتر انجام خواهد پذیرفت . همچنین مشخص خواهد شد که کدامیک از بخش های سیستم در خلال امن سازی , به درستی مورد بررسی قرار نگرفته و آنطور که باید , تدابیر امنیتی در مورد آن پیاده سازی و رعایت نشده است.

بمنظور انجام یک بررسی امنیتی و تست نفوذپذیری که بتواند کل سیستم و مجموعه را به چالش بکشد , نیاز به یک پلان و برنامه عملکرد کامل , دقیق و در عین حال موثر میباشد . با توجه به اینکه بررسی های امنیتی و تست های نفوذ پذیری اغلب توسط نیروی انسانی بانجام می رسد (ابزار های بررسی خودکار نیز بر اساس روش های کاری نیروی انسانی طراحی میگردند) , مواردی که در انجام این امور می باست رعایت شده و مد نظر قرار گیرند در قالب تجارب افراد مجری پدیدار میگردند . این تجربیات و چک لیست ها بصورت فهرست وار مورد استفاده قرار میگیرند , تحت عنوان " متدولوژی تست نفوذ " شناخته میشوند .

شرکت در طی ۱۲ مرحله اقدام به بررسی و اجرای تست نفوذپذیری می نماید که در ادامه توضیحاتی در مورد هر مرحله آورده شده . تصویری که در ادامه مشاهده میگردد , چرخه انجام تست نفوذ پذیری را به ترتیب انجام آن نشان میدهد .



۱-۲. جمع آوری اطلاعات

جمع آوری اطلاعات اولین مرحله در انجام تست نفوذپذیری میباشد . در این مرحله اقدام به جمع آوری اطلاعات راجع به سیستم/سازمان/مجموعه تحت بررسی میشود و از نتایج این مرحله برای ورود به مراحل بعد استفاده میگردد . با توجه به محدود بودن پارامتر زمان در انجام تست های نفوذ , این مرحله بسیار مهم میباشد و همواره سعی میگردد تا حداکثر اطلاعات ممکن و مفید راجع به هدف کسب گردد. بدین منظور هم از روش های فنی (DNS/Who Is) و هم از روش های غیر فنی مانند search engine ها , گروه های خبری , لیست های پستی و ... استفاده میگردد . بطور کلی اغلب این اطلاعات از طریق اینترنت کسب میگردند اما محدود به آن نیستند . در این مرحله نیازی به کسب اطلاعات و یا برقراری تماس مستقیم با هدف نمیباشد و همه اطلاعات بطور غیر مستقیم جمع آوری میگردند .

۲-۲. ترسیم نقشه شبکه

در این مرحله بدنبال اطلاعاتی که از فاز اول بدست آمده , اطلاعات مربوط به منابع شبکه هدف جدا شده و مورد بررسی و پویش دقیقتر قرار میگیرند . بر اساس اطلاعات موجود اقدام به شناسایی سیستم های فعال در سازمان شده , و نحوه ارتباطات این سیستم ها با هم شناسایی و مورد بررسی قرار میگیرند . در این مرحله که اصطلاحاً Foot Printing خوانده میشود از لحاظ فنی شبکه هدف شناسایی میگردد .

از جمله مواردی که در این مرحله انجام می شود میتوان به این موارد اشاره کرد :

- شناسایی سیستم های فعال شبکه
- شناسایی پورت های باز و سرویس های فعال
- ترسیم نقشه لایه خارجی شبکه (فایروال ها , روترها , ...)
- شناسایی سرویس های دارای ریسک بالا
- تشخیص سیستم های عامل سیستم های موجود
- شناسایی مسیر های عبور داده ها به مقاصد مختلف (**network routes**)
- شناسایی قوانین فایروال ها
- شناسایی جزئیات سرویس های مجود (**Service fingerprinting**)

۳-۲. شناسایی نقاط ضعف

قبل از شروع این مرحله , بررسی کننده میباست نقاطی را برای انجام حمله به هدف انتخاب نماید .در خلال مرحله شناسایی ضعف ها , بررسی کننده فعالیت های زیادی را برای تشخیص نقاط ضعف قابل استفاده برای نفوذ انجام میدهد . این فعالیت ها شامل موارد زیر میباشند :

- تشخیص سرویس های آسیب پذیر بر اساس banner های جمع آوری شده در مرحله قبل
- انجام پویش آسیب پذیری های امنیتی (Vulnerability Scan)
- بررسی ضعف های به اشتباه گزارش شده و ضعف های موجود ولی گزارش نشده (false positive & false negative verification)
- تهیه لیستی از آسیب پذیری های شناسایی شده
- تخمین اثرات آسیب های شناسایی شده و دسته بندی آنها
- شناسایی روش های استفاده از ضعف ها و آماده سازی سناریو های نفوذ بر اساس آنها

۴-۲. نفوذ

در این مرحله بررسی کننده تلاش میکند تا با استفاده از نتایج مراحل قبل و مشکلات شناسایی شده , از راهکارهای امنیتی موجود سیستم ها عبور کرده و دسترسی هرچه بیشتر را فراهم نماید. این مرحله خود میتواند به بخش های زیر تقسیم گردد :

- **جستجوی ابزار/کد های Proof Of Concept برای آسیب پذیری ها :**

شناسایی کدها و ابزارهای موجود برای استفاده از ضعف های امنیتی شناسایی شده , موجود در آرشیو خصوصی و یا آرشیو ها و منابع عمومی . در صورتی که منبع مورد نیاز در آرشیو خصوصی موجود بوده و قبلاً ار صحت عملکرد آن اطمینان حاصل شده میتوان اقدام به استفاده از آن نمود . در غیر اینصورت منابع/کد ها و ابزار های یافته شده در محیط ایزوله و شبیه سازی شده مطابق شرایط و سیستم های هدف , آزمایش میگردد

- **تولید ابزار / اسکریپت های مورد نیاز :**

در مواردی بنا بر شرایط , بررسی کننده میبایست اقدام به تولید ابزار ها و اسکریپت های مورد نیاز خود نماید . از جمله این دلایل میتوان به عدم وجود ابزارهای مناسب و کارآمد و یا صرفه جویی در هزینه ها اشاره کرد .

- **آزمایش ابزارها/اسکریپت ها**
  - ایجاد تغییرات لازم در کد/ابزارهای PoC
  - آزمایش کد/ابزار های PoC در یک محیط مجزا شده

- **استفاده از کد/ابزارها علیه اهداف :**

اقدام به استفاده نهایی ازکدها و ابزارهای آزمایش شده در شرایط واقعی علیه اهداف شناسایی شده برای ایجاد دسترسی و نفوذ هرچه بیشتر در سیستم های تحت بررسی

- **بررسی و یا حذف آسیب پذیری از لیست موجود** (بدلیل غیر قابل استفاده بودن) :

تنها با استفاده از آسیب پذیری ها این امکان برای بررسی کننده فراهم میگردد تا اقدام به تایید یک ضعف امنیتی و شناسایی آن نماید.

- **مستند سازی نتایج حاصل شده :**

کلیه فعالیت های انجام شده در طی این مرحله مستند سازی شده و لیستی از آسیب پذیری ها و اثرات آنها و سیستم های آسیب پذیر و قابل استفاده برای نفوذ با استفاده از این ضعف ها تهیه میگردد .

۵-۲. ایجاد و ارتقا سطوح دسترسی

در هر شرایطی اقدام به جمع آوری اطلاعات و نفوذ بیشتر در سیستم ها توسط بررسی کننده ممکن میباشد . بررسی کننده در این حال اقدام به تهیه مستنداتی درمورد آسیب پذیریها و ریسک های تآیید شده پرداخته و احتمال انجام حملات خودکار (Automated) را علیه کل مجموعه بررسی نماید.

۱-۵-۴) فراهم کردن دسترسی اولیه :

فراهم کردن دسترسی های اولیه به سیستم از طریق بدست آوردن دسترسی های سطح پایین در سیستم ها میباشد که راه های مختلفی برای انجام آن وجود دارد , از قبیل :

- کشف ترکیب username/password ها از طریق حلات dictionary attack و Brute force علیه سیستم ها
- کشف نام های کاربری بدون کلمه عبور و یا کلمات عبور پیش فرض در سیستم
- کشف سرویس های عمومی (public) که امکان انجام اعمال خاصی از قبیل خواندن/نوشتن/تغییر فایل ها بر روی سیستم را فراهم میکند.

۲-۵-۴) دستیابی به سطوح متوسط و عادی دسترسی

۳-۵-۴) تصاحب سیستم ها :

این مرحله شامل ایجاد دسترسی به تمامی سیستم هایی میباشد , که برای دستیابی به سیستم/هدف/دسترسی/اطلاعات نهایی به آنها نیاز میباشد . این سیستم های عادی میتوانند شامل روترها , سوئیچ ها , سرورهای DNS و ... باشند.

۴-۵-۴) تصاحب و دسترسی نهایی به سیستم :

در این مرحله بررسی کننده به هدف/سیستم/اطلاعات نهایی در سیستم دست میابد و کنترل کل سیستم را در دست میگیرد.

۶-۲. جمع آوری مجدد اطلاعات

- اقدام به حملات مجدد بر روی کلمات عبور برای دستیابی به نام های کاربری بیشتر (sniffing/crack)
- Sniff کردن ترافیک شبکه و آنالیز آن
- جمع آوری آدرس های E-Mail ...
- شناسایی شبکه ها و مسیر های عبور (Routes)
- ترسیم نقشه از شبکه داخلی
- تکرار مراحل فوق برای سیستم هایی که طی این مرحله تحت کنترل بررسی کننده درآمده است.

۷-۲. دسترسی به اطلاعات مورد نظر

بررسی کننده ، پس از نفوذ به کلیه سیستم های مورد نیاز (ممکن) اقدام به جستجو و دریافت/کنترل اطلاعات خاص مینماید . بعنوان مثال در طی نفوذ به شبکه یک بانک , بررسی کننده در این مرحله اقدام به استخراج اطلاعات مشتریان بانک و یا تغییر در آنها (در صورت درخواست) مینماید .

۸-۲. پایدارسازی دسترسی

بررسی کننده پس از اتمام مراحل فوق , میباست دسترسی خود به سیستم ها و شبکه (داخلی) را پایدار نماید تا برای دسترسی مجدد به یک سیستم نیاز به استفاده مجدد از نقاط ضعف که برای نفوذ اولیه مورد استفاده قرار گرفته , نباشد . بررسی کننده با نصب Back Door بر روی سیستم های تحت کنترل این عمل را انجام میدهد. همچنین ولی میتواند اقدام به نصب Root Kit بر روی سیستم های تحت کنترل نماید تا علاوه بر پایدار کردن دسترسی , از تشخیص دسترسی توسط کنترل کننده گان اصلی سیستم نیز جلوگیری بعمل آورد .

۹-۲. از بین بردن ردپاها

بررسی کننده در این مرحله اقدام به از بین بردن کلیه رد پاهایی مینماید که از خود در طول مراحل قبل , در سیستم ها و شبکه بر جای گذاشته است . این مرحله به بررسی کننده کمک میکند تا از دید مدیران سیستم ها و شبکه مورد بررسی پنهان مانده و بتواند دسترسی خود (و ادامه نفوذ) را حفظ نماید .

۱۰-۲. ممیزی

در برخی موارد ممیزی (Audit) سیستم , میتوانند اطلاعات مفید بیشتری را راجع به نقاط ضعف سیستم ها دهند که تست نفوذ پذیری به تنهایی قادر به تشخیص همه این موارد نمیباشد . بنابر این ممیزی سیستم ها میبایست بعد از اتمام تست های نفوذ پذیری

صورت گیرند .ممیزی های سیستم ها میبایست مجددا مواردی از قبیل پورت های باز , سرویس های فعال , ارتباطات برقرار شده , دسترسی های File System , رویداد نگاری (Logging) و ... را در برگیرند .

۱۱-۲. تهیه گزارش

در طول اجرای هر آزمون امنیتی،گزارشهای ذیل آماده ودر پایان هر مرحله بررسی ارائه خواهد شد:

گزارش ضعفها با درجه خط بالا:

مطابق یک روال روزانه یا طبق نیاز مشتری،تیم امنیتی ،گزارشی درباره ضعفهای کشف شده با درجه بالای خطر،که تهدید مستقیمی را متوجه ساختار اطلاعاتی مجموعه میکند، ارائه خواهد داد. این گزارش بصورت مکتوب یا از طریق email رمزگذاری شده ارائه خواهد شد.

گزارش نهایی:

پس از پایان آزمون امنیتی، تیم امنیتی، گزارش نهایی ارائه خواهد کرد.

خلاصه پروپوزال:

فرایند فوق در طول حدود ۶۰ روز کاری و به مدد یک تیم دو تا سه نفره از زبده ترین کارشناسان بنام که هر یک در یک فیلد تخصصی فعالیت مینمایند، انجام خواهد شد. یک نفر بعنوان کارشناس امن سازی سیستم عامل و سامانه های نرم افزاری تحت وب معرفی خواهد شد. یک نفر بعنوان کارشناس امن سازی شبکه و در صورت نیاز یک نفر نیز جهت امن سازی ارتباطات رادیویی. بخشی از عملیات بصورت حضور در محل دانشگاه و بخشی نیز بصورت ریموت صورت می پذیرد. تمامی سرورهای مجازی دانشگاه، و ۲۲ سامانه نرم افزاری، وب سایت و سرویس هایی که در دانشگاه فعال هستند مانند سرویس ایمیل، هات اسپات، پشتیبان گیری و ... در حیطه کاری فرایند مذکور دیده شده اند. پس از ارائه گزارش آسیب پذیریها در حیطه های مذکور، مراحل هاردنینگ انجام خواهد شد. در پیش فاکتور ارائه شده توسط این شرکت به شماره:۹۷۱۳۸۶۷/پ، فیلد اول تا اینجا به پایان خواهد رسید.

در راستای نیاز آن دانشگاه به خدمات نگهداشت امنیت شبکه و سامانه های نرم افزاری و ... این شرکت در فیلد دوم پیش فاکتور ۲۴ جلسه مشاوره امنیتی در طول یک سال بعبارتی دوبار در ماه در نظر گرفته است. در راستای تکمیل فرایند نگهداشت امنیتی، دو مرحله تست نفوذ پذیری به فاصله ۶ ماه یکبار و در مجموع ۲ بار انجام خواهد شد که این مهم در فیلد سوم پیش فاکتور این شرکت گنجانده شده است.

(پایان)