Server Hardening

مقاوم سازی ویندوز سرور

مقاوم سازی سیستم

مقاوم سازی سیستم‌ها مجموعه‌ای از ابزارها، تکنیک‌ها و به روش‌ها برای کاهش سطح آسیب‌پذیری در برنامه‌های کاربردی فناوری اطلاعات، سیستم‌ها، زیرساخت‌ها، سیستم‌عامل‌ها و سایر زمینه‌ها است. هدف از هاردنینگ یا مقاوم سازی سیستم‌ها کاهش ریسک امنیتی با حذف بردارهای احتمالی و متراکم‌تر کردن سطح حمله سیستم است. با حذف برنامه‌های اضافی، عملکردها و دسترسی‌های اضافی حساب‌ها، پورت‌های بدون استفاده، مجوزها، دسترسی‌ها و ...، مهاجمان سایبری و بدافزارها فرصت کمتری برای بدست آوردن جای پایی در اکوسیستم فناوری اطلاعات سازمان خواهد داشت. هاردنینگ سیستم‌ها نیازمند یک رویکرد هوشمند و روشمند برای ممیزی، شناسایی، بستن و کنترل آسیب‌پذیری‌های امنیتی بالقوه در سراسر سازمان است. انواع مختلفی از فعالیت‌های هاردنینگ سیستم وجود دارد، از جمله: هاردنینگ نرم‌افزار، هاردنینگ سیستم‌عامل، هاردنینگ سرور، هاردنینگ نقاط پایانی، هاردنینگ دیتابیس و هاردنینگ شبکه .

یکی از پراستفاده از سیستم‌عامل‌های مورد استفاده در سازمان‌ها، Microsoft Windows Serverاست. این سیستم‌عامل به دلیل امکانات زیادی که به مدیران شبکه می‌دهد، یکی از محبوب‌ترین‌هاست. از طرفی به همین دلیل هم، محبوب مهاجمین سایبری و هکرها نیز هست و آنها با استفاده از آسیب‌پذیری‌هایی که از این سیستم‌عامل و سرویس‌های آن منتشر می‌شود، برای نفوذ به شبکه سازمان استفاده می‌کنند. به همین موضوع هاردنینگ این سیستم‌عامل از مواردی است که هر مدیر شبکه‌ای باید با دقت آن را پیگیری و پیاده‌سازی کند.

: Server Hardening

فرآیند امنیتی که برای امن سازی سرورهای ویندوزی و لینوکسی انجام می شود و درجه امنیتی آنها را بالا می برد به عنوان Server Hardening شناخته می شود. در واقع سرور هاردنینگ یا مقاوم سازی سرور به مجموعه پردازش هایی برای بهبود امنیت پیکربندی های سرور اشاره می کند.

❖ اهمیت هاردنینگ ویندوز سرور

به گفته‌ی مایکروسافت، سطح امنیت یک سازمان بر همه‌ی اعضا و زیرمجموعه‌های آن سازمان تاثیر دارد. هرگونه ریسک که احتمال وقوع یک حمله‌ی امنیتی را فراهم می‌کند، می‌تواند بسیار خطرناک باشد و همه‌ی امور عادی و روزمره‌ی سازمان را مختل یا متوقف کند.

سرور ویندوز یک هدف نرم برای مهاجمان است اگر:

- *فایل های سیستم عامل از یک منبع غیر قابل اعتماد نصب می شوند.*
- *سیستم با وصله ها امنیتی جدید به روز رسانی نشده باشد.*
- *حساب‌های مدیر دارای پسوردهای ضعیف باشند.*
- *سیستم های فایل از NTFS استفاده نمی کنند و رمزگذاری نشده هستند.*

حمله‌ی هکر به سرور با تحقیق و شناسایی نقاط ضعف سیستم انجام می‌شود و پس از شناسایی نقاط نفوذ، به دنبال راه‌هایی می‌گردد که هدفش را هرچه سریع‌تر محقق کند اجرای چک لیست هاردنینگ ویندوز سرور، با افزایش سطح امنیت سرور و رفع نقاط ضعف سیستم، از وقوع بسیاری حملات جلوگیری می‌کند و هنگام بروز هرگونه تهاجمی، با ارتقای علایم هشداردهنده‌ی مختلف، حمله را شناسایی کرده و بدین شکل فرصت بیش‌تری برای خنثی کردن حمله در اختیارتان قرار می‌دهد. نهایتا با حذف سیستم‌های آسیب‌دیده، به شما کمک می‌کند به بهترین شکل به حمله مهاجمان پاسخ دهید.

❖ پیکربندی و تنظیمات کاربران در ویندوز سرور

با این‌که نسخه‌های جدید ویندوز سرور، شما را به تغییر رمزعبور Administrator مجبور می‌کنند، اما باز نیاز است رمزعبور خود را تغییر دهید. علاوه‌براین، از آن‌جایی که حساب ادمین (که سطح دسترسی بسیار بالایی دارد) یک هدف محبوب برای حمله‌ی مهاجمان است و از طرف دیگر در شرایط بسیار محدودی به آن نیاز دارید، بهتر است گزینه‌ی ورود با این امکان را به‌طور کامل غیرفعال کنید تا از سواستفاده از آن جلوگیری شود.

اگر اکانت مدیر لوکال را غیرفعال کنید، باید یک حساب مدیریت جدید راه‌اندازی شود. توجه داشته باشید که حساب‌های کاربری را با دسترسی‌های مورد نیاز برای هر نقش ایجاد کرده و برای همه‌ی حساب‌ها از رمزعبورهای قدرت‌مند استفاده کنید تا مطمئن شوید که حساب‌های موجود در سرور به خطر نمی‌افتند. در استاندارد بودن و قوی بودن پسوردهای مدیریتی و سیستمی‌تان حساس و سخت‌گیر باشید، به‌ویژه برای اکانت‌های مدیریتی که سطح دسترسی بالایی دارند.

به‌طور کلی توصیه می‌شود اکانت‌های مهمان(Guest Account)غیرفعال باشند و فقط هنگام ضرورت یا نیاز آن‌ها را فعال کنید. همه‌ی اکانت‌های داخلی فرصتی برای نفوذ به‌شمار می‌آیند و اکانت‌های مهمان در میان آن‌ها بالاترین میزان خطر و نفوذپذیری را به خود اختصاص می‌دهند.

به‌طور کلی، در تنظیمات امنیتی حساب کاربری به این موارد توجه کنید:

- **پیچیدگی و طول**: مشخص کنید که رمزعبور قوی از نظر شما باید دارای چه مشخصاتی باشد. هر رمزعبور باید دست‌کم ۱۵ کاراکتر داشته و ترکیبی از حرف، عدد، علایم خاص و کاراکترهای نامرئی باشد. هم‌چنین توصیه می‌شود از کلمات معنادار یا لغت‌نامه‌ای استفاده نشود.
- **انقضای رمزعبور**: مشخص کنید مدت‌زمان اعتبار هر رمزعبور چه مدت است. همه‌ی پسوردها را دست‌کم هر ۹۰ روز یکبار عوض کنید.
- **تاریخچه‌ی گذرواژه**: مشخص کنید مدت زمان استفاده‌ی دوباره از رمزهای عبور قبلی چه‌قدر است.
- **قفل حساب**: مشخص کنید که بعد از چند تلاش با رمزعبور ناموفق، حساب کاربر باید تعلیق شود.

گذرواژه‌های قدیمی عامل بسیاری از هک‌های موفق هستند، بنابراین مطمین شوید که با تغییر منظم رمزعبور، در برابر این موارد از سرور محافظت می‌کنید.

حساب‌های کاربری بدون استفاده را به‌سرعت غیرفعال یا حذف کنید.

به تنظیمات پیش‌فرض در سطح دسترسی هر اکانت یا گروه‌های تعریف شده توجه داشته باشید و سطح دسترسی به عملکردهای مهم و حیاتی را به حداقل برسانید. برای مثال، به‌طور پیش‌فرض، حق «دسترسی به یک رایانه از شبکه» به گروه Everyone اعطا می‌شود. که عملا به همه‌ی کاربران امکان دسترسی نامحدود از راه دور به پوشه‌های مشترک داده می‌شود.

سیاست‌های گروهی (Group Policy) برای مسدودسازی اکانت‌ها را براساس بهترین شیوه‌های پیشنهادشده تنظیم کنید.

به کاربران اجازه ایجاد اکانت مایکروسافتی و لاگین در کامپیوترها را ندهید.

❖ ویژگی‌های ویندوز و پیکربندی نقش‌ها

مایکروسافت از نقش‌ها و ویژگی‌ها برای مدیریت بسته‌های سیستم‌عامل استفاده می‌کند. نقش‌ها اساسا مجموعه‌ای از ویژگی‌ها هستند که برای یک هدف خاص طراحی شده‌اند، بنابراین به‌طور کلی می‌توان نقش‌های متناسب با یک سرور را انتخاب و سپس ویژگی‌های مورد نظر را از آن‌جا سفارشی کرد.

در این مرحله دو کار مهم وجود دارد که باید انجام دهید:

۱) مطمئن شوید هر آن‌چه نیاز دارید نصب شده است. برای مثال ممکن است برای عملکرد صحیح برنامه‌های‌تان به یک نسخه‌ی فریم‌ورک دات‌نت یا IIS نیاز داشته باشید، مواردی که بدون آن‌ها برنامه‌های شما کار نخواهند کرد. هم‌چنین نرم‌افزاری نصب کنید که یکپارچگی فایل‌های مهم سیستم‌عامل را بررسی کند. ویندوز قابلیتی موسوم به Resource Protectionدارد که فایل‌های مهم خاص را به‌طور خودکار بررسی و هر کدام را که معیوب بود با نسخه‌ی سالم جایگزین می‌کند.
۲) هر چیزی که نیاز ندارید را حذف کنید. برنامه و بسته‌های اضافی و غیرضروری، امنیت سرور را کاهش می‌دهند و باید حذف شوند. این اقدام، برای برنامه‌های پیش‌فرض و از پیش نصب شده‌ی روی سرور نیز ضروری است. سرورها باید با توجه به میزان نیاز و ضرورت طراحی شوند، به‌گونه‌ای که بخش‌های لازم به‌راحتی و سریع‌تر عمل کنند.

❖ به‌روزرسانی پیوسته

بهترین راه برای حفظ امنیت سرور، به‌روز نگه داشتن آن است. با این‌که ویندوز سرور، پیکربندی امنی دارد اگر می‌خواهید هم‌چنان امن بماند، حتما آن را به‌روز نگه دارید. باید در نظر داشته باشید که بیش‌تر نقاط آسیب‌پذیری که مورد سواستفاده‌ی هکرها و مهاجمان قرار می‌گیرند، بیش از یک سال قدمت دارند. مطمئن شوید که هر به‌روزرسانی امنیتی ضروری فوراً نصب شده باشد. هرچه سریع‌تر یک وصله امنیتی جدید را اعمال کنید، سریع‌تر می‌توانید آسیب‌پذیری‌ها را برطرف کنید و از خود در برابر آخرین تهدیدات شناخته شده محافظت کنید.

مشاغلی که از نسخه های قدیمی ویندوز استفاده می کنند بیشتر در معرض خطر هستند. به عنوان مثال، مایکروسافت پشتیبانی از ویندوز ۷ را در ژانویه ۲۰۲۰ پایان داد، بنابراین هر کسی که هنوز از آن استفاده می کند در معرض خطر حملات جدید قرار دارد. بنابراین، مهم است که اطمینان حاصل کنید که سیستم عامل شما قبل از قرار گرفتن در معرض آسیب پذیری ها ارتقا یافته است.

توجه داشته باشید نرم‌افزارهای ضدویروس و ضدجاسوس‌افزار از جمله مواردی هستند که باید به‌طور مستمر مورد نصب، فعال‌سازی و به‌روزرسانی قرار بگیرند.

❖ پیکربندی فایروال

فایروال ویندوز یک نرم‌افزار داخلی مناسب است که امکان پیکربندی ترافیک مبتنی بر پورت را از داخل سیستم‌عامل فراهم می‌کند. در یک سرور مستقل یا هر سرور بدون فایروال سخت‌افزاری، فایروال ویندوز، سرور را با محدود کردن سطح حمله به پورت‌های مجاز، در برابر حملات مبتنی بر شبکه محافظت می‌کند.

❖ پیکربندی دسترسی از راه دور

اگر از RDP استفاده می‌کنید مطمین شوید که فقط از راه VPN قابل دسترسی است چون باز گذاشتن RDP فرصت حمله و نفوذ هکرها به سرور شما را فراهم می‌کند. بنابراین مطمین شوید که RDP فقط به‌وسیله‌ی کاربران مجاز قابل دسترسی است.

نقطه ضعف Remote Desktop این است که مهاجمان می توانند از دسترسی از راه دور برای کنترل سیستم شما سوء استفاده کنند و اطلاعات حساس را سرقت کنند یا بدافزار نصب کنند. قابلیت دسترسی از راه دور به طور پیش فرض غیرفعال است و پس از فعال شدن می توانید به راحتی آن را غیرفعال کنید. اطمینان حاصل کنید که هر زمان که کاربران به طور فعال از آن استفاده نمی کنند، این ویژگی را خاموش کنید.

علاوه‌برRDP ، اگر از مکانیسم‌های مختلف دسترسی از راه دور دیگری مانند PowerShell و SSH استفاده می‌کنید اطمینان پیدا کنید که فقط از راه VPN قابل دسترسی هستند و با دقت قفل شده‌اند. به‌هیچ‌وجه نباید از Telnet استفاده کرد، زیرا اطلاعات را به‌شکل متن ساده ارسال می‌کند و بسیار ناامن است.

❖ پاورشل

مایکروسافت PowerShell را برای فعال کردن مدیریت خودکار سیستم از طریق یک رابط یکپارچه توسعه داده ایجاد کرده است. این زبان برنامه نویسی قدرتمند یکی از ویژگی های اصلی جعبه ابزار مدیریت سیستم است، زیرا در همه جا حاضر است و به شما اجازه می دهد تا به راحتی محیط Microsoft Windows خود را کنترل کنید. متأسفانه، مهاجمان نیز می توانند از این روش برای کنترل کامل سیستم شما سوء استفاده کنند.

به صورت خاص، نسخه های قبلی PowerShell به دلیل آسیب پذیری های امنیتی خطرناک هستند، بنابراین باید PowerShell 2.0و کمتر را از سیستم عامل خود حذف کنید.

❖ آنتی ویروس

یک آنتی ویروس برای شبکه های با هر اندازه ضروری است. هنگامی که آنتی ویروس را نصب می کنید، به یاد داشته باشید که برای به روز رسانی خودکار پیکربندی شده است. آنتی ویروس بدون امضای ویروس(signatures) به روز شده بی فایده است.

❖ پشتیان‌گیری از اطلاعات و سیستم

یکی از مهم‌ترین اقدامات برای هاردنینگ ویندوز سرور، پشتیبان‌گیری منظم از سیستم‌عامل ویندوز سرور و داده‌های ذخیره‌شده در آن است. زیرا این اقدام، حمله‌ی باج‌افزارها به ویندوز سرور را کاهش می‌دهد. بک‌آپ‌گیری به شما کمک می‌کند تا هنگام حمله‌ی باج‌افزارها، اطلاعات را به‌راحتی بازیابی کنید.

در نهایت، از سیستم‌عامل‌هایتان ایمیج بگیرید تا همه‌ی نرم‌افزارهای نصب‌شده و همه‌ی تنظیمات امنیتی که اعمال کرده‌اید در فایل ایمیج کپی شوند. در این شرایط اگر نیاز داشته باشید که ویندوز سرور را دوباره نصب کنید همه‌ی برنامه‌ها و تنظیمات امنیتی پیشین از روی فایل ایمیج روی ویندوز سرور پیاده می‌شود و دیگر نیازی نیست پس از نصب ویندوز جدید، همه نرم‌افزارها و تنظیمات امنیتی موردنیازتان را دوباره یک‌به‌یک اعمال کنید.

<<نمونه چک لیست های امنیتی سرور >>

➢ چک لیست امنیتی وب سرور IIS

۱) به هیچ عنوان سروری که بصورت کامل فرآیند Hardening بر روی آن انجام نشده است را به اینترنت متصل نکنید.
۲) سرور را در محل فیزیکی امن قرار بدهید ، امنیتی فیزیکی از اولین مواردی است که در حوزه امنیت بایستی رعایت شود.
۳) به هیچ عنوان وب سرور IIS را بر روی Domain Controller نصب نکنید.
۴) بر روی وب سرور IIS هرگز پرینتر نصب نکنید.
۵) بر روی سرور دو عدد کارت شبکه بگذارید ، یکی برای مدیریت سرور و دیگری برای کاربران.
۶) حتما Service Pack ها ، Patchها و البته Hotfix های لازم را بر روی سیستم عامل سرور نصب کنید.
۷) ابزار IIS Lockdown را بر روی سرور وب اجرا کنید (در IIS های قدیمی و ویندوزهای سرور قدیمی)
۸) ابزار امنیتی URLScan را بر روی وب سرور نصب و اجرا و پیکربندی کنید.
۹) حتما برای Remote Desktop از Encryption مناسب استفاده کنید.
۱۰)حتما برای Remote Desktop قابلیت های Account Lockout و Session Timeout را قرار بدهید.
۱۱)هرگونه سرویس بلااستفاده بر روی سیستم عامل ویندوز را غیرفعال کنید.
۱۲)مطمئن شوید که همگی سرویس ها با حداقل دسترسی کاربری اجرا می شوند.
۱۳)اگر به سرویس های FTP ، SMTPو NNTP نیازی ندارید آنها را غیرفعال کنید یا حذف کنید.
۱۴)سرویس Telnet را حتما غیرفعال و از روی سیستم عامل حذف کنید.
۱۵)اگر سرویس وضعیت ASP.NET یا ASP.NET State Service توسط Application های شما استفاده نمی شود آن را غیرفعال کنید.
۱۶)اگر از WebDAV استفاده نمی کنید یا مطمئن هستید Application های شما از آن استفاده نمی کنند آن را غیرفعال کنید.
۱۷)اگر از WebDAV استفاده می کنید حتما پارامترهای امنیتی آن را رعایت کنید.
۱۸)قسمت Data Access Components را فقط در صورت نیاز نصب کنید در غیر اینصورت حذف کنید.
۱۹)قسمت MS Index Server را فقط در صورت نیاز نصب کنید و اگر نیازی نیست نصب نکنید.
۲۰)گزینه HTML Version از قسمت Internet Service Manager را اصلا فعال یا نصب نکنید.
۲۱)قسمت MS FrontPage Server extensions را فقط در صورت نیاز نصب کنید در غیر اینصورت حذف کنید.
۲۲)فرآیند Hardening را برای TCP/IP Stack هم انجام بدهید.
۲۳)پروتکل های NetBIOS و SMB را غیرفعال کنید ، پورتی های ۱۳۷ ، ۱۳۸ ، ۱۳۹ و ۴۴۵ را مسدود کنید.
۲۴) Policyهای مربوط به Recycle Bin و Paging File System را مجددا پیکربندی کنید به تناسب سرور.
۲۵)تنظیمات امنیتی CMOS را انجام دهید.
۲۶)امنیت فیزیکی مربوط به CD-ROM و USB Drive ها و ... را فراهم کنید.

➢ چک لیست امنیتی Account ها یا حساب های کاربری

۱) هرگونه حساب کاربری اضافه و بلااستفاده را از روی سرور حذف کنید.
۲) حساب کاربری Guest را غیرفعال کنید.
۳) نام کاربر Administrator را عوض کنید و یک پسورد قوی برای آن انتخاب کنید.
۴) حساب کاربری IUSR_MACHINE را در صورتیکه Application ای از آن استفاده نمی کند غیرفعال کنید.
۵) یک حساب کاربری با دسترسی محدود برای anonymous account ها ایجاد کنید البته در صورتیکه این سرویس را نیاز دارید.
۶) به هیچ عنوان به کاربر anonymous دسترسی بصورت write بر روی محتوای دایرکتوری ها و اجرای دستورات بر روی سرور ندهید.
۷) اگر بر روی سرور شما چندین Web Application وجود دارد برای هر کدام کاربر anonymous جداگانه ای تعریف کنید.
۸) دسترسی های حساب کاربری process های ASP.NET را با کمترین سطح دسترسی ممکن تعریف کنید.
۹) گزینه قبل زمانی کاربردی است که شما از اکانت پیشفرضی که برای سرویس ASP.NET تعریف شده است استفاده نمی کنید.
۱۰)از یک Password Policy قوی برای کلیه اکانت های موجود بر روی سرور استفاده کنید.
۱۱)دسترسی Remote را به حداقل ممکن برسانید ، گروه Everyone را از قسمت Access this computer from networkحذف کنید.
۱۲)برای هر کدام از Administrator های سرور یک اکانت جداگانه تعریف کنید و اکانت مشترک ایجاد نکنید.
۱۳) Null Sessionرا غیرفعال کنید یا به بیانی دیگر Anonymous Logon را غیرفعال کنید.
۱۴)برای تفکیک کردن اکانتها و کاربردهایشان حتما بایستی تاییدیه دریافت شود (هر شخص نتواند به شخص دیگری دسترسی بدهد).
۱۵)در گروه Administrators بیشتر از دو کاربر تعریف شده نداشته باشید.
۱۶)فقط اجازه Logon بصورت Local را بدهید یا برای Remote Desktop حتما از رمزنگاری استفاده کنید.

➢ چک لیست امنیتی فایل ها و پوشه ها

۱) همیشه چند عدد پارتیشن بر روی هارد دیسک ایجاد کنید.
۲) هیچوقت Home Directory مربوط به وب سرور را در پارتیشن سیستم عامل قرار ندهید.
۳) بر روی پارتیشن هایی که فایل سیستم آن NTFS است فایل ها و پوشه های خودتان را قرار بدهید.
۴) محتویات هر وب سایت را در پوشه ای به غیر از Home Directory وب سرور قرار بدهید که NTFS هم باشد.
۵) همیشه یک وب سایت جدید ایجاد کنید و وب سایت پیشفرض یا Default Site را غیرفعال کنید.
۶) از وب سرور بصورت متناوب لاگ برداری کنید و لاگها را مرتب بررسی کنید.

۷) فایل های Log وب سرور را در پارتیشنی به غیر از پارتیشنی که محتویات وب سایت در آن قرار دارند قرار بدهید . (NTFSباشد)
۸) دسترسی گروه Anonymous و Everyone به پوشه های system32 و پوشه وب سایت ها را محدود کنید.
۹) مطمئن شوید که دایرکتوری ریشه یا Root Directory وب سرور به کاربران گروه Anonymous به هیچ عنوان دسترسی نداده باشد.
۱۰)مطمئن شوید که دایرکتوری هایی که شامل محتویات اطلاعاتی وب سرور هستند به کاربران گروه Anonymous به هیچ عنوان دسترسی نداده باشند.
۱۱)در هر دو مورد گذشته ترجیحا از گزینه Deny برای Access Control Entry های Permission ها استفاده کنید.
۱۲)قابلیت Remote IIS Administration یا Remote WWW Administration را به همراه سرویس آن غیرفعال و یا حذف کنید.
۱۳)تمامی ابزارهای Resource Kit به همراه SDK ها را از روی وب سرور حذف کنید.
۱۴)تمامی Sample Application ها یا برنامه های پیشفرض مثل وب سایت پیشفرض IIS را حذف کنید. (از جمله صفحات Help)
۱۵)آدرس IP را از Header حذف کنید. (برای جلوگیری از شناسایی محل یا Content Location)

➢ چک لیست امنیتی Share های شبکه

۱) تمامی Share های بلااستفاده از جمله Administrative share ها را از بین ببرید.
۲) حتما دسترسی ها را به افراد مجاز بدهید و هیچوقت گروه everyone را در لیست دسترسی ها قرار ندهید.
۳) توجه کنید که سیستم های مانیتورینگی مثل SCOM و SCCM از سری System Center با Administrative Shareها کار می کنند.
۴) فقط پورت های مورد استفاده در File and Printer Sharing را در فایروال باز کنید.
۵) دسترسی به شبکه اینترنت را فقط از طریق پورت های ۸۰ و در صورت نیاز ۴۴۳ مجاز کنید.
۶) حتما استفاده از اینترنت را محدود کنید و فقط از پروتکل های امنی مثل SSL برای دسترسی به اینترنت استفاده کنید.
۷) اگر تعداد استفاده کنندگان از Share ها مشخص است ، محدودیت Concurrent Connections بر روی Shareها بگذارید.

➢ چک لیست امنیتی Registry

۱) سرویس Remote Registry را غیرفعال کنید و یا دسترسی به آن را محدود کنید.
۲) برای سرورهای Standalone فایل SAM را حتما امن کنید و در تنظیمات رجیستری NoLMHash را فعال کنید.

۳) حتما قابلیت های Auditing و Logging را بر روی سرورها فعال کنید.
۴) حتما Failed Logon Attempts را Audit کنید.
۵) محل Log فایل های IIS را تغییر بدهید.
۶) هر چند وقت یکبار Log ها را آرشیو و تجزیه و تحلیل کنید. (حدالمقدور قسمت های امنیتی لاگ ها را)
۷) حداکثر اندازه لاگ فایل را تعریف کنید.
۸) دسترسی به فایل Metabase.bin را همیشه Audit کنید.
۹) تنظیمات IIS را به گونه ای انجام دهید که قالب W3C Extended Log File نیز بازرسی یا Audit شود.
۱۰)بصورت متناوب از رجیستری خودتان Backup تهیه کنید.

- **چک لیست امنیتی Site ها و Virtual Directory ها**

۱) هیچگاه وب سایت ها را بر روی پارتیشن سیستم ایجاد نکنید.
۲) تنظیمات Parent Path را غیرفعال کنید.
۳) Virtual Directoryهای خطرناکی مثل IISSamples و IISAdmin و IISHelp و Scripts را حذف کنید.
۴) Virtual Directoryمربوط به MSADC را حذف کنید.
۵) Virtual Directoryبه نام IIS Internet Printing را حذف کنید.
۶) مطمئن شوید که Certificate های سرور معتبر و به روز هستند.
۷) از هر Certificate فقط برای کاری که برای آن تعریف شده است استفاده کنید.
۸) مطمئن شوید که Public Key مربوط به Certificate ای که دریافت کرده اید معتبر است.
۹) مطمئن شوید که Certificate مورد استفاده شما Revoke نشده باشد.
۱۰) ISAPI Filterهای بلااستفاده را از روی سرور حذف کنید.