بسمه تعالی

مرکز آپا دانشگاه محقق اردبیلی

کارگاه آموزشی

امن سازی وب سرور ویندوز

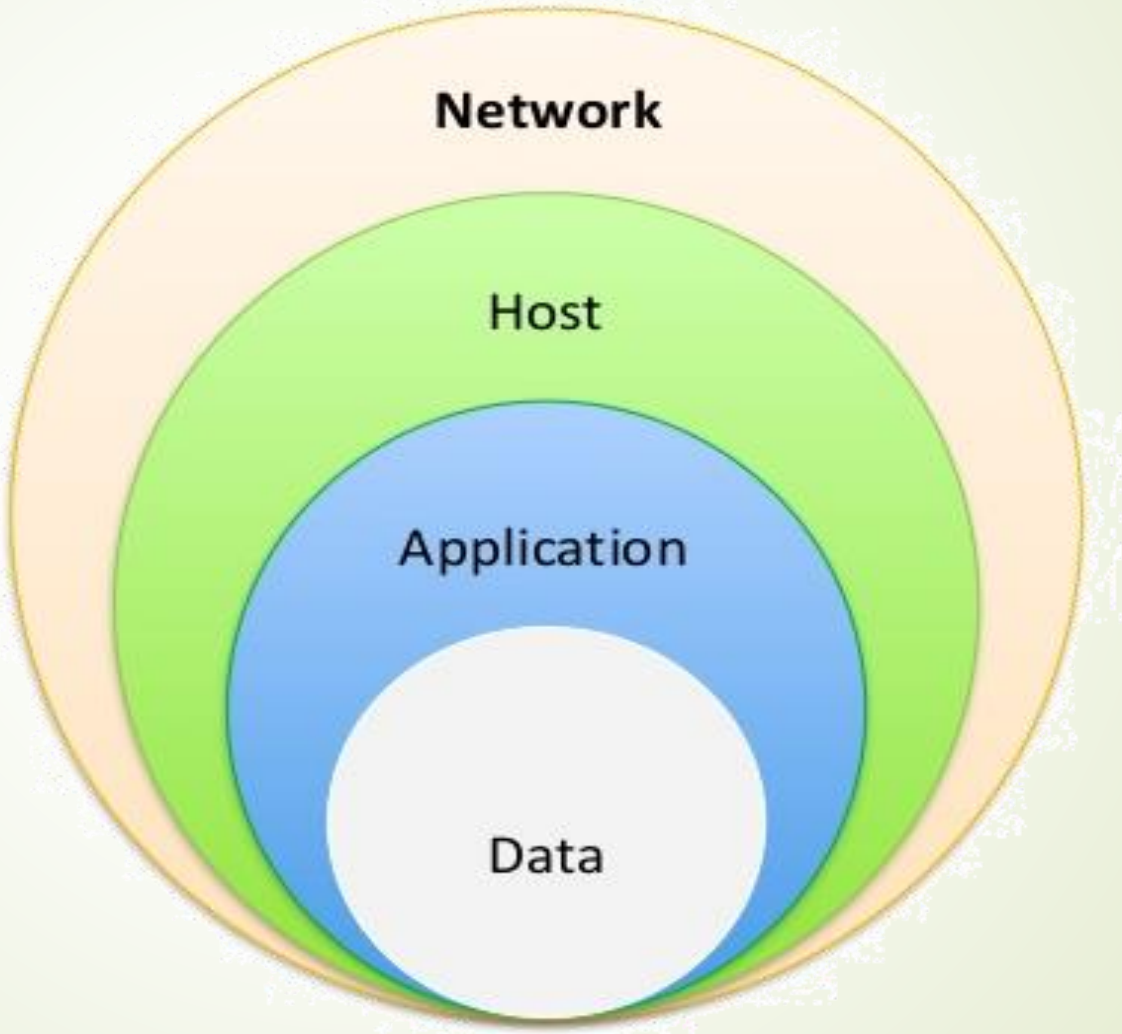
توسط:

علی النقی مصطفائی

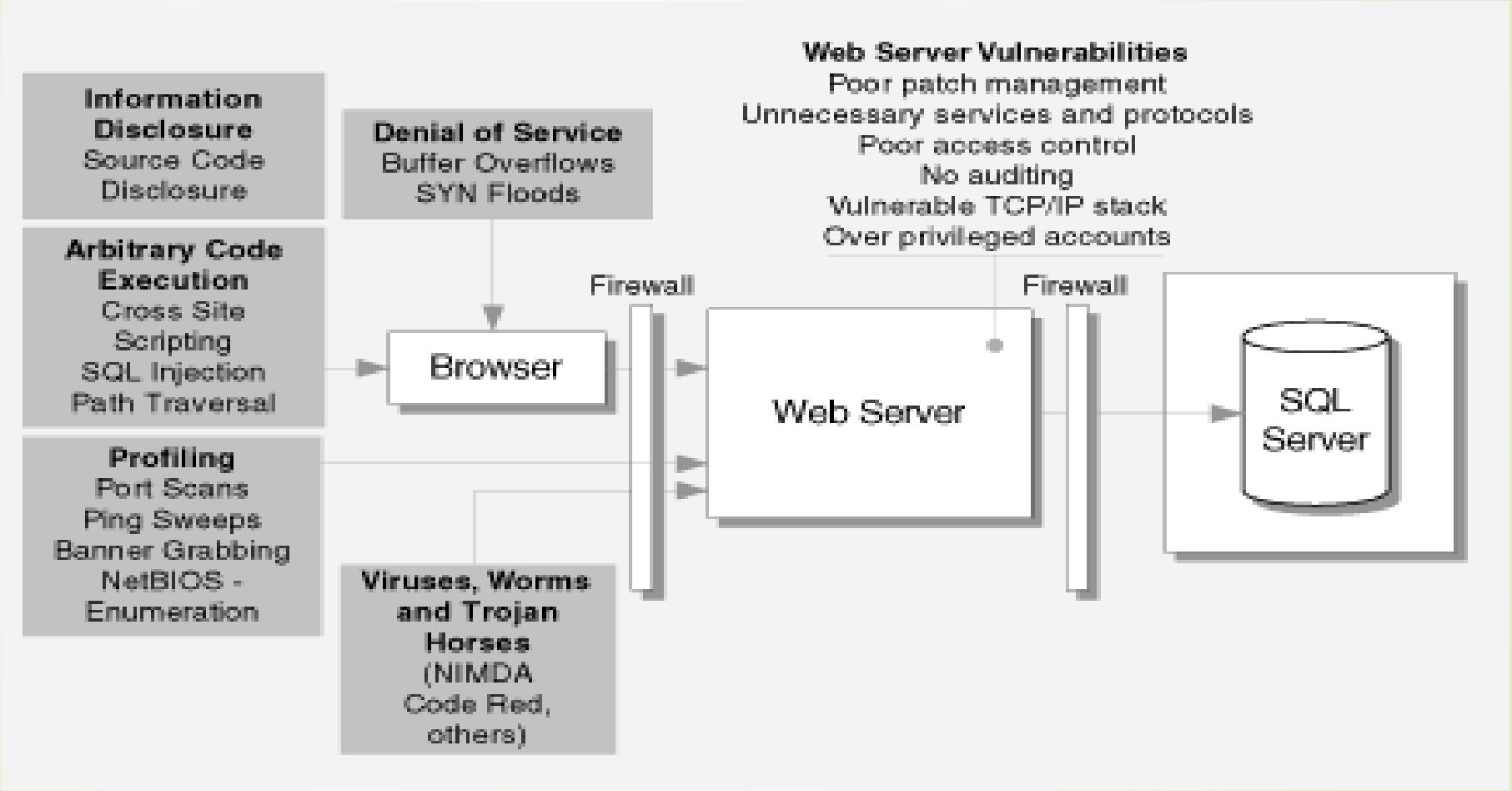
mostafa@uma.ac.ir

مرداد ۱۳۹۶

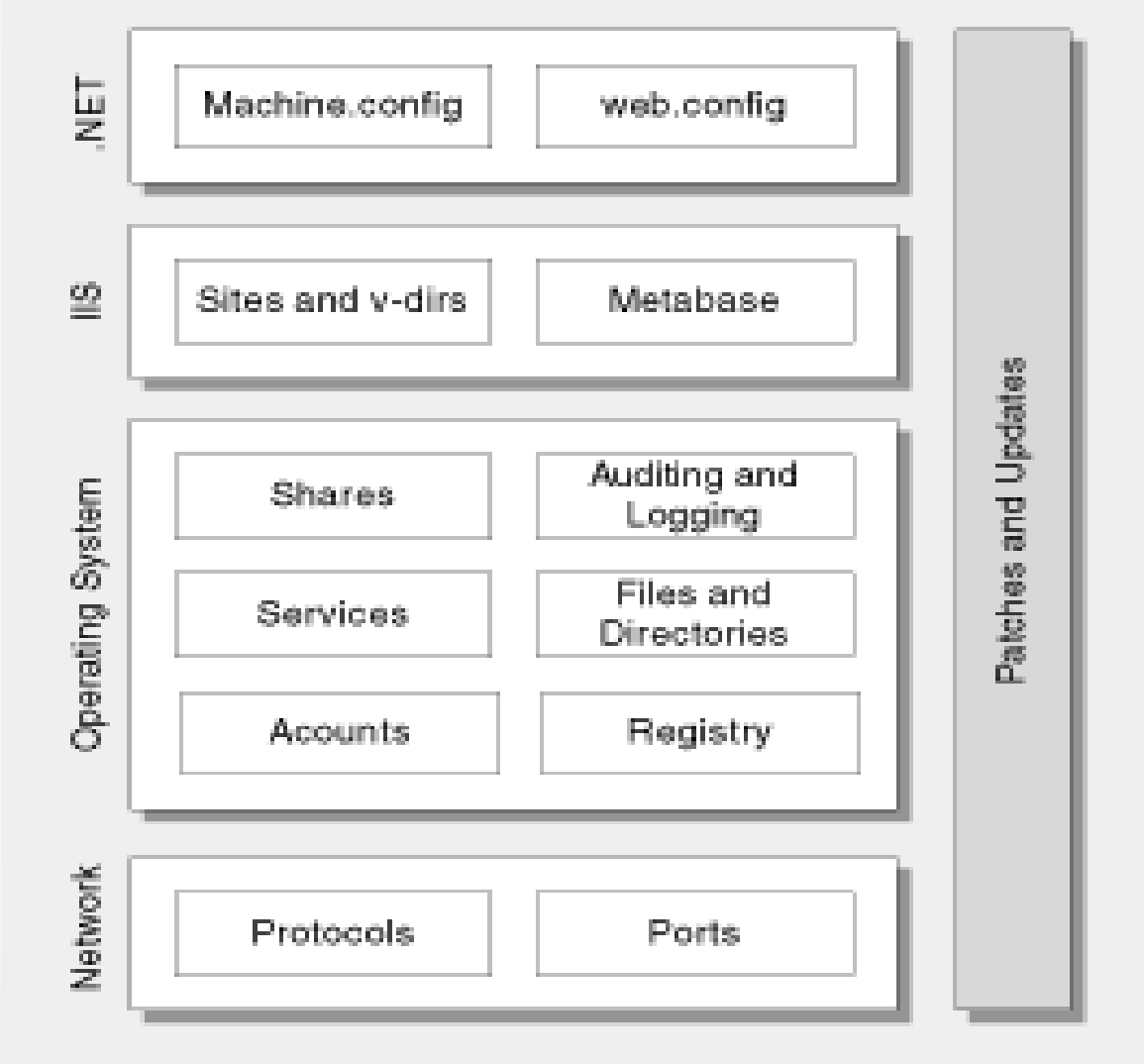
مقدمه ای بر امنیت لایه بندی



تهدیدهای وب سرور



دسته بندی تنظیمات امنیتی



مراحل امن سازی وب سرور ویندوز

- بخش اول: اقدامات کلی و اولیه
- بخش دوم: سیاست های امنیتی مربوط به تنظیمات شبکه
  ۱- پروتکل ها ۲- پورت ها
- بخش سوم: سیاست ها و تنظمیات امنیتی مربوط به سیستم عامل
- بخش چهارم: تنظیمات امنیتی مربوط به سرویس IIS

بخش ۱: اقدامات کلی و اولیه

- ✓ گام ۱: وب سرور در بستر سخت افزاری مناسب نصب گردد.
- ✓ گام۲: امنیت فیزیکی سرور و پورت های فیزیکی سرور
- ✓ گام ۳: عدم استفاده از نسخه های منسوخ سیستم عامل ویندوز که امکان بروزرسانی ندارد.
- ✓ گام ۴: نصب کلیه Patch های امنیتی ویندوز و .NET FrameWork.
- ✓ گام ۵: نصب آنتی ویروس معتبر و بروزرسانی مداوم آن
- ✓ گام ۶: فعال کردن فایروال وتنظیم مناسب آن
- ✓ گام ۷: عدم اتصال به اینترنت در صورتیکه که نیازی به اتصال به اینترنت نیست.
- ✓ گام ۸: درصورت نیاز به اتصال اینترنت بر روی سرور اینکار را بعد از اتمام فرایند امن سازی انجام دهید.

مرحله۲: سیاست های امنیتی مربوط به تنظیمات شبکه

- ✓ گام ۱: پروتکل های غیر ضروری وبلا استفاده را از روی سرور حذف کنید.
- ✓ گام ۲: در صورتیکه از پروتکل WebDAV استفاده نمی کنید آن را غیرفعال کنید.

گام۳: پروتکل NetBIOS و SMB را غیرفعال کنید.

نحوه

- ✓ پورتهای ۱۳۷،۱۳۸،۱۳۹و ۴۴۵(مربوط بهNetBIOS وSMB) را ببندید.
- ✓ تمام پورتها به غیراز پورت ۸۰ و ۴۴۳ را ببندید.
- ✓ در صورتیکه از پروتکل https استفاده نمی کنید پورت ۴۴۳ را هم ببندید.

نحوه غیرفعال کردن NetBIOS

- Right-click **My Computer** on the desktop, and click **Manage**.
- Expand **System Tools**, and select **Device Manager**.
- Right-click **Device Manager**, point to **View**, and click **Show hidden devices**.
- Expand **Non-Plug and Play Drivers**.
- Right-click **NetBios over Tcpip**, and click **Disable**.

نحوه غیرفعال کردن SMB

- Right-click on **Local Area Connection**, and click **Properties**.
- Clear the **Client for Microsoft Networks** box.
- Clear the **File and Printer Sharing for Microsoft Networks** box

SMB uses the following ports:

TCP port 139

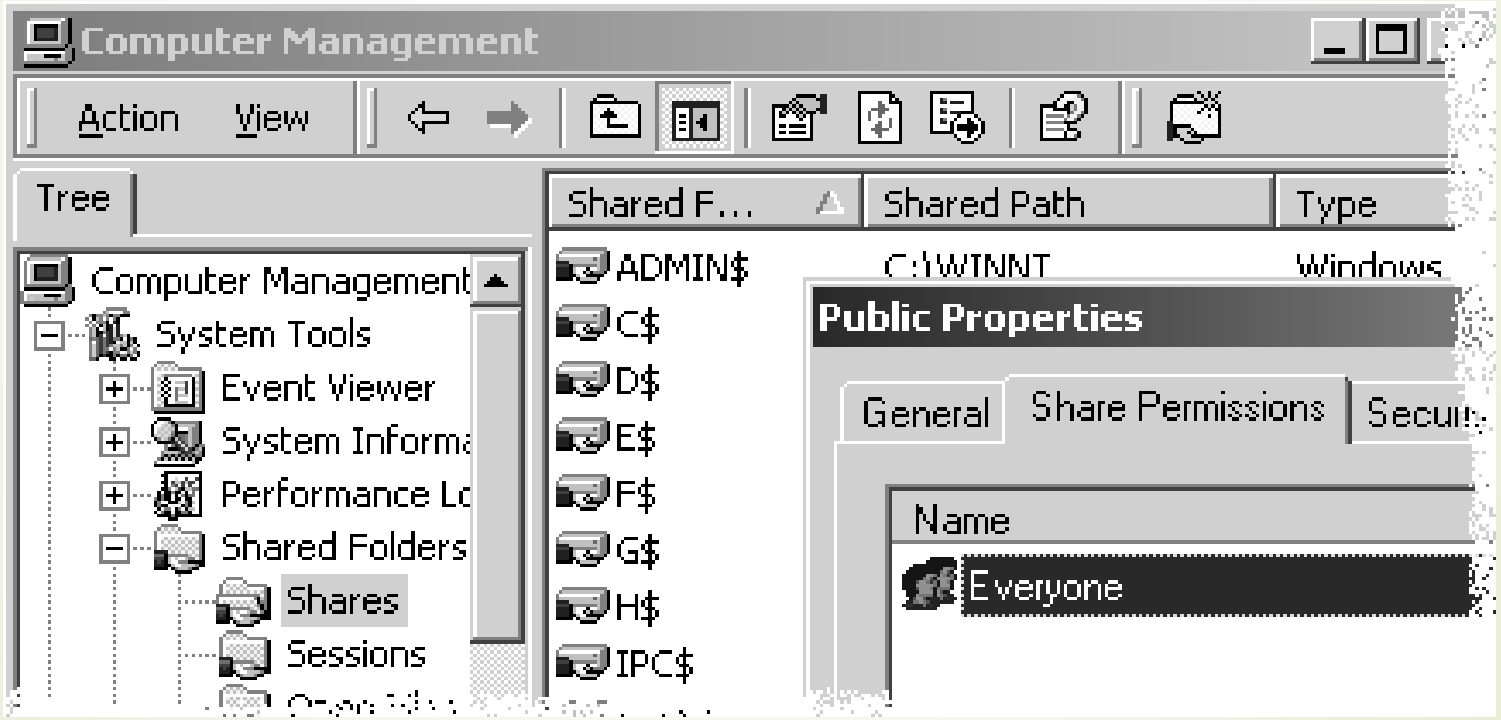
TCP port 445

سیاست ها و تنظیمات امنیتی مربوط به سیستم عامل

1. سیاست های امنیتی مربوط به shares
2. سیاست های امنیتی مربوط به اکانت ها
3. سیاست های امنیتی مربوط به سرویس ها
4. سیاست های امنیتی مربوط به لاگ ها
5. سیاست های امنیتی مربوط به فایل ها ودایرکتوری ها
6. تنظیمات مربوط به رجیستری

۱- سیاست های امنیتی مربوط به shares

- ✓ حذف share های غیرضروری و حتی administrative shares
- ✓ اعمال مجوزهای NTFS بر روی share های ضروری
  حذف گروه everyone از لیست دسترسی ها



۲- سیاست های امنیتی مربوط به اکانت ها

- ✓ حذف یا غیرفعال کردن اکانت های بلااستفاده
- ✓ غیر فعال اکانت guest
- ✓ تغییر نام اکانت Administrator
- ✓ اعمال Password Policy قوی:
  - طول و پیچیدگی (حداقل ۸ کاراکتر ترکیبی)
  - تاریخ انقضای پسورد(حداقل ۴۲ روز)
- ✓ در قسمت Access this computer from the network حذف everyone

۲- سیاست های امنیتی مربوط به اکانت ها

- ✓ غیرفعال کردن Null sessions به منظور جلوگیری از Anonymous logon به سیستم
  HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- ✓ از ارائه اکانت مشترک به افراد خودداری کنید(اکانت مجزا برای هر فرد)
- ✓ اگر چند Admin مختلف درسیستم دارید برای هر کدام اکانت مجزا ایجاد کنید.
- ✓ تعداد Adminها بیشتر از ۲ نفر نباشد.
- ✓ اگر بر روی سرور چندین Web Applicationوجود دارد برای هر کدام کاربر anonymous جداگانه ای تعریف گردد.

۳- سیاست های امنیتی مربوط به سرویس ها

- ✓ سرویس های غیرضروری و بلااستفاده حذف گردد.
- ✓ سرویس ها با حداقل مجوز های لازم اجرا شوند.
- ✓ سرویس Telnetرا حتما غیرفعال و از روی سیستم عامل حذف کنید.
- ✓ اگر سرویس ASP.NET State (aspnet_state.exe) توسط Applicationهای شما استفاده نمی شود آن را غیرفعال کنید.

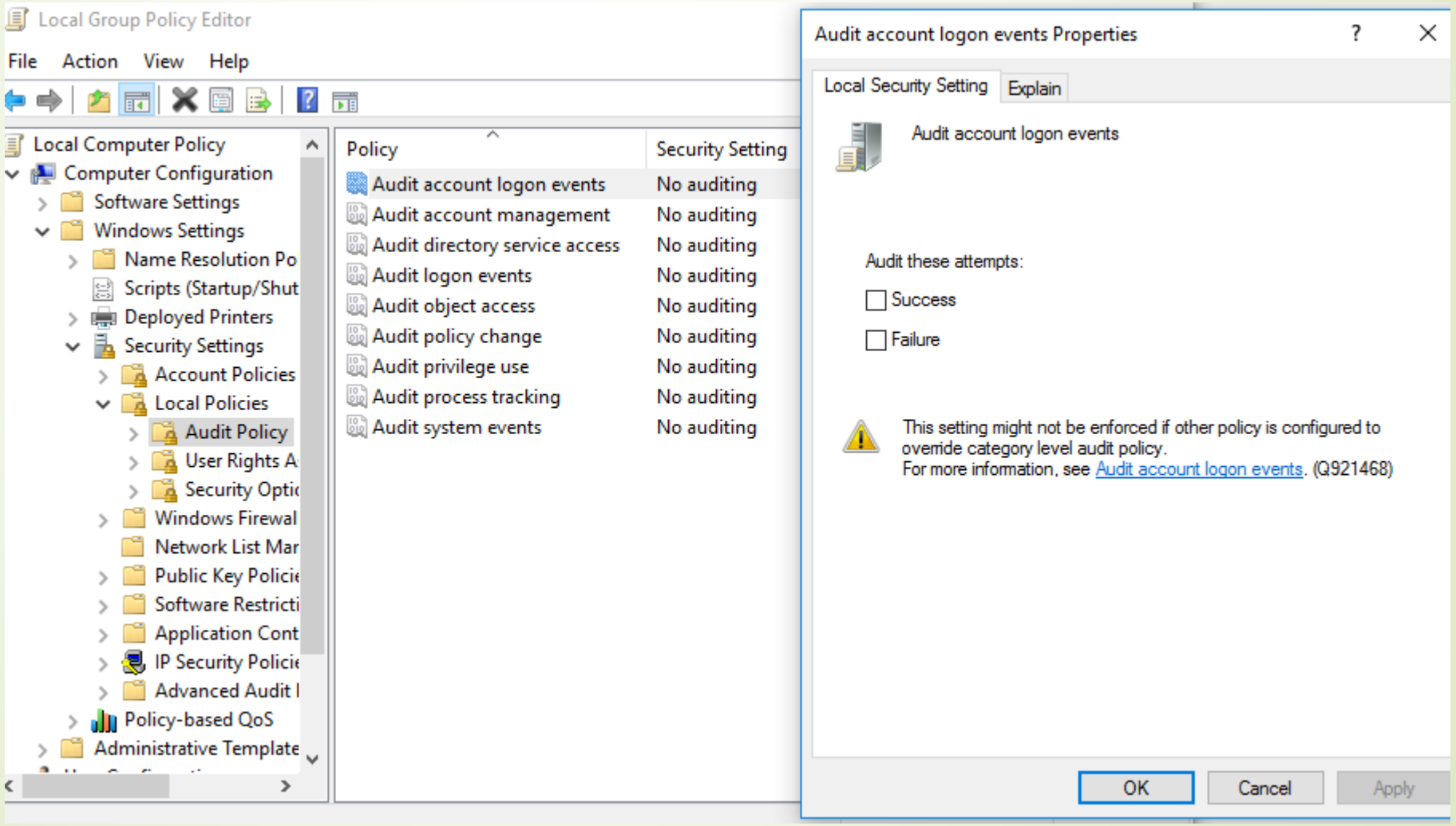
```
<sessionState  mode="Off " />
```

٤- سیاست های امنیتی مربوط به لاگ ها

- ✓ تمام login های موفق و ناموفق لاگ شود.(نحوه فعال کردن)
  ۵۳۱: log on using a disabled account
  ۵۲۹: invalid user or password
  ۵۲۸: success logon
- ✓ محل لاگ IIS عوض شده و توسط مجوزهای NTFS امن شود.
- ✓ فایلهای لاگ IIS نه در پارتیشن سیستم عامل باشد و نه در پارتیشن وب
- ✓ لاگ ها را آرشیو کرده و به صورت آفلاین بررسی کنید.
- ✓ بسته به نیاز حداکثر اندازه لاگ فایل را تعریف کنید.
- ✓ دسترسی به فایل Metabase.binرا همیشه Auditکنید.
- ✓ تنظیمات IISرا به گونه ای انجام دهید که قالب W3C Extended Log Fileنیز بازرسی یا Audit شود.

نحوه فعال کردن لاگ مربوط به login ها

Local Policies →Audit Policy→Audit account logon events



۵- سیاست های امنیتی مربوط به فایل ها ودایرکتوری ها

- ✓ دایرکتوری مربوط به وب سرور را در پارتیشن سیستم عامل قرار ندهید.
- ✓ با استفاده از مجوزهای NTFS امکان دسترسی به system tools و دایرکتوری وب برای گروه everyone را حذف کنید.

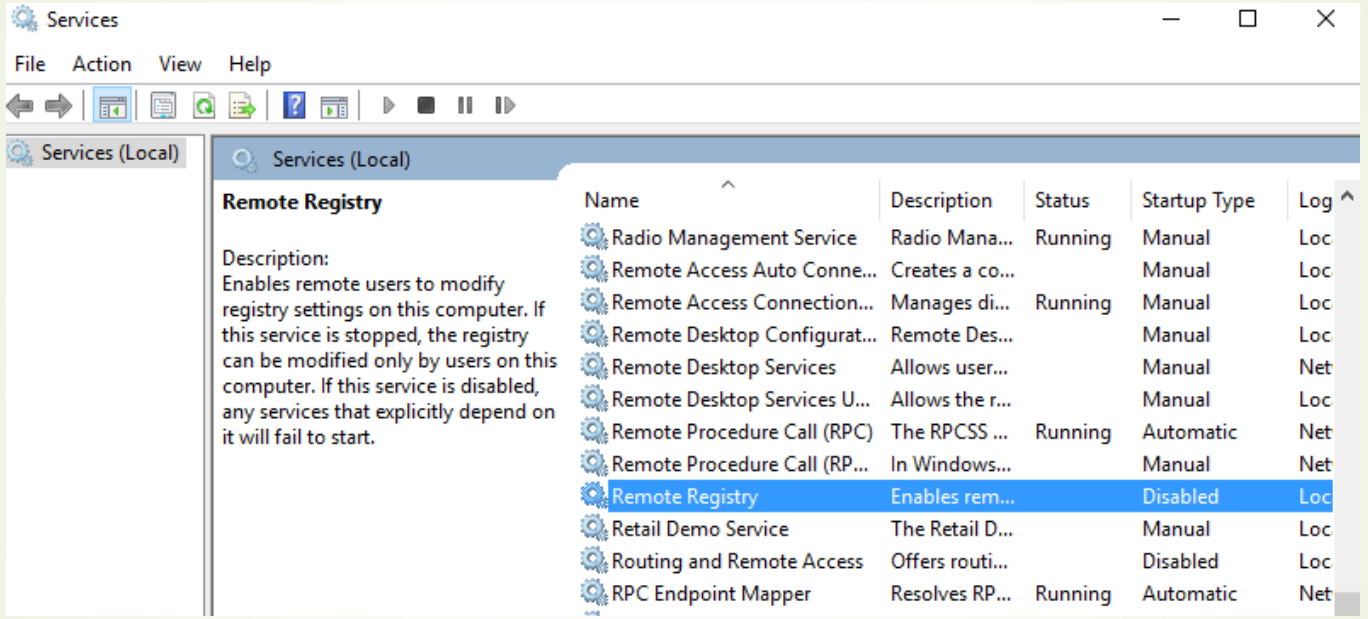
  \%system%\system32, \..\Microsoft.NET\Framework\{version}, \inetpub*
- ✓ بر روی کلیه محتویات دایرکتوری وب مجوز write را برای اکانت های anonymous را Deny کنید.

۵- سیاست های امنیتی مربوط به فایل ها ودایرکتوری ها

- ✓ تمامی Tools ها و Resource Kit و SDKها را از روی وب سرور حذف کنید.
- ✓ قابلیت Remote IIS Administration را حذف کنید.
  %SystemDrive%\System32\inetsrv\iisadmin
- ✓ تمام sample Application ها راحذف کنید.
  \Inetpub\IISSample و %SystemDrive%\Help\IISHelp

٦- تنظیمات امنیتی مربوط به رجیستری

✓ سرویس Remote Registryرا غیرفعال کنید.



✓ بصورت متناوب از رجیستری Backup تهیه کنید.

سیاستهای امنیتی مربوط به IIS

- ✓ وب سایت ها را بر روی پارتیشن سیستم ایجاد نکنید.
  در محل پیش فرض \inetpub\wwwroot قرار ندهید.
- ✓ تنظیمات Parent Pathرا غیرفعال کنید. (نحوه انجام)
- ✓ Virtual Directoryهای خطرناکی مثل IISSamplesو IISAdminو IISHelpو Scriptsرا حذف کنید.
- ✓ حذف یا امن سازی (RDS(Remote Data Services. (نحوه انجام)
  Virtual Directoryمربوط به MSADCرا حذف کنید.
- ✓ Virtual Directoryبه نام IIS Internet Printingرا حذف کنید.
- ✓ بازبینی و تنظیم WEB Permissions(**Script source access, Write , Execute , Read**)

سیاستهای امنیتی مربوط به IIS

- ✓ قسمت MS FrontPage Server extensionsرا فقط در صورت نیاز نصب کنید در غیر اینصورت حذف کنید.(جلوگیری از توسعه از راه دور)
- ✓ قسمت Data Access Components(MDAC) را فقط در صورت نیاز نصب کنید در غیر اینصورت حذف کنید. (جلوگیری از توسعه از راه دور)
- ✓ قسمت MS Index Serverرا فقط در صورت نیاز نصب کنید و اگر نیازی نیست نصب نکنید.
- ✓ ISAPI Filterهای بلااستفاده و غیرضروری را از روی سرور حذف کنید.

parent paths نحوه غیرفعال کردن

This IIS metabase setting prevents the use of ".." in script and application calls to functions such as **MapPath**. This helps guard against **directory traversal attacks.**

To disable parent paths

- ✓ Start IIS.
- ✓ Right-click the root of your Web site, and click **Properties**.
- ✓ Click the **Home Directory** tab.
- ✓ Click **Configuration**.
- ✓ Click the **App Options** tab.
- ✓ Clear **Enable parent paths**.

نحوه حذف RDS

Removing RDS

If your applications do not use RDS, remove it.

To remove RDS

- ✓ Remove the /MSADC virtual directory mapping from IIS.
- ✓ Remove the RDS files and subdirectories at the following location:
- ✓ \Program Files\Common Files\System\Msadc
- ✓ Remove the following registry key:
- ✓ HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch

با تشکر از توجه شما