بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

امن سازی DHCP Server

گروه زیر ساخت امن

تیرماه ۱۳۹۳

فهرست مطالب

۱. مقدمه

سرورهای DHCP[۱] به طور خودکار آدرس‌های IP، به کلاینت‌ها و سایر ابزارهای شبکه اختصاص می‌دهند. همچنین DHCP توانایی اختصاص زیرشبکه، DNS ، Gateway و دیگر تنظیمات کلاینت‌های عضو شبکه را دارد. در این مستند تدابیر امنیتی که می‌توان به سرور DHCP اعمال نمود تا آن ها را در برابر حملات حفاظت کرد، ارائه می‌شود.

قبل از مطالعه و اجرای این سند، نکات زیر باید مورد توجه قرار گیرد:

- از آن‌جا که ممکن است تنظیمات امن‌سازی، کارکردهای سیستم را مختل یا غیرفعال کند، لازم است قبل از اجرای تنظیمات، یک نسخه پشتیبان از پیکربندی سیستم تهیه شود.
- برای اجرای الزامات تعیین شده در این سند، اولویت با خط‌مشی‌های سازمان است. به عبارت دیگر اگر برخی از الزامات بیان شده در این سند، با خط‌مشی‌های سازمان تداخل یا تضاد داشت، اولویت با خط‌مشی‌های سازمان است.
- در تهیه این سند، سعی شده است که حداکثر الزامات مرتبط با حوزه‌ی سند، پوشش داده شود. اما این بدان معنا نیست که پس از اجرای این الزامات، سیستم به صورت صد در صد امن خواهد بود. الزامات بیان شده در این سند، حداقل انتظارات برای امن‌سازی در حوزه‌ی تعریف شده در این مستند است.

۱,۱ تعاریف و مفاهیم

پیش از شروع، لازم است تا مفهوم حفاظت دسترسی به شبکه[۲] مختصرا توضیح داده شود.

---

[۱] Dynamic Host Configuration Protocol

[۲] -Network Access Protection

حفاظت دسترسی شبکه (NAP): تکنولوژی ارائه شده توسط مایکروسافت به منظور کنترل دسترسی است. استفاده از حفاظت دسترسی شبکه، مدیران شبکه سازمان‌ها را قادر می‌سازد تا سیاست‌های کنترلی برای الزامات سلامت سیستم ها تعریف کنند. به عنوان نمونه‌ای از الزامات سلامت سیستم، می‌توان به کنترل نصب آخرین به روزرسانی‌ها، کنترل نصب آخرین نسخه به‌روز شده آنتی ویروس اشاره کرد. تحت حفاظت دسترسی شبکه، کلاینت‌ها بایستی سلامت و امنیت سیستم خود را پیش از دریافت آدرس IP و دسترسی گرفتن به شبکه اثبات نمایند. این تکنولوژی تنها از آدرس‌های IP نسخه ۴ پشتیبانی می‌کند.

۱,۲تهدیدات مربوط به سرورهای DHCP

سرورهای DHCP مستعد قرار گرفتن در معرض بسیاری از حملات امنیتی هستند. از جمله مهمترین حملات به این دسته از سرورها می‌توان به DHCP Starvation و سوء استفاده از Rogue DHCP اشاره نمود.

- DHCP Starvation

این حمله با انتشار درخواست DHCP با آدرس MAC جعلی اتفاق می‌افتد. اگر به تعداد کافی از این نوع درخواست، ارسال شود مهاجم می‌تواند فضای آدرس در دسترس سرورهای DHCP را برای مدت زمان معینی پرکند. این حمله به سادگی SYN flooding است.

- Rogue DHCP

یک سرور DHCP است که توسط مهاجم یا یک کاربر ناآگاه روی شبکه برپاشده و تحت کنترل مدیران شبکه نیست. معمولا می‌تواند یک مودم یا یک روتر با قابلیت DHCP باشد، که کاربر به صورت ناآگاهانه به شبکه اضافه کرده است. چنین سیستم‌هایی می‌توانند توسط مهاجمین جهت انجام حملاتی مانند man in the middle و sniffing مورد استفاده قرار گیرند. مهاجم با استفاده از یک سرور Rogue DHCP می تواند به اطلاعات شبکه نظیر آدرس کلاینت‌ها دسترسی پیدا کند. از آنجا که پاسخ DHCP

معمولا شامل سرور DNS و default gateway است، مهاجم می‌تواند سیستم خودش را به عنوان default gateway و سرورDNS جا بزند.

به منظور تعیین سطح حملات، تشخیص موارد زیر الزامی است:

- فایل‌های نصب شده: فایل هایی که به عنوان بخشی از نقش سرور DHCP نصب شده‌اند.
- سرویس‌های در حال اجرا: سرویس‌هایی که به عنوان بخشی از نقش سرور DHCP نصب شده‌اند.
- قوانین فایروال: قوانین فایروال که سرور DHCP استفاده می‌کند.
- وابستگی‌های نقش: وابستگی‌های موجود در وظایف سرور DHCP

۱,۳ دامنه

توصیه‌های ارائه شده در این مستند قابل بکارگیری بر روی کلیه سرورهای DHCP مایکروسافت می‌باشد.

۲. امن سازی

این بخش به ارائه معیارهای امنیتی می‌پردازد که اعمال آن‌ها در پیکربندی سرور DHCP منجر به حفاظت بیشتر در برابر انواع حملات خواهد شد.

۲,۱تخصیص یک کامپیوتر مجزا جهت اجرای نقش DHCP سرور

ترکیب چندین نقش سروری روی یک سیستم تنها در شرایط خاص توصیه می‌شود. زیرا سطح حملات احتمالی را افزایش می‌دهد. بنابراین توصیه می‌شود که سرور DHCP تنها برای این منظور اختصاص داده شده و سرویس دیگری روی آن ارائه نشود. حتی اگر این سرویس همراه با سایر سرویس ها ارائه می‌شود، اکیدا توصیه می‌گردد که نقش سروری DHCP همراه با سرویس‌هایی مانند وب سرورها،

سرویس صدور گواهی [۳] ، سرویس دامنه Active Directory[۴] و سرویس دسترسی از راه دور که اغلب مورد هدف مهاجمین قرار می‌گیرند استفاده نشود.

۲,۲ نصب windows server 2008 core

در صورت استفاده از ویندوز سرور توصیه می‌شود از windows server 2008 core installationاستفاده گردد، این نوع از نصب باعث می‌شود تا هیچ کدام از فایل ها و سرویس‌های مربوط به توابع گرافیکی ویندوز (GUI) نصب نشده و همین امر موجب کاهش احتمال حملات می‌شود. با استفاده از نصب windows server 2008 core، تنها می‌توان سیستم را به صورت محلی و با استفاده از خط فرمان، مدیریت نمود. برخی دستورات لازم در این زمینه در بخش اعمال تنظیمات ارائه شده است. لازم به توضیح است در صورتی که از core installation استفاده نگردد نیز همچنان می‌توان از سایر گزینه‌های امن‌سازی استفاده نمود.

۲,۳ حذف سیستم های Rogue DHCP

یکی از شکل‌های معمول حملات استفاده از سرورهای DHCP Rogue است که آدرس کلاینت‌ها را ارسال می‌کنند. با افزودن یک سرور DHCP به شبکه به سادگی می‌توان این نوع از حملات را راه اندازی نمود.

به منظور جلوگیری از فعالیت سرورهای DHCP غیر قابل اعتماد، ویندوز سرور ۲۰۰۸ در Active Directory از قابلیتAuthorization پشتیبانی می‌کند و سیستم هایی که بخشی از domain هستند، ابتدا باید از Active Directory Domain مجوز داشته باشند.

---

[۳] - Active directory Certificate Service

[۴] - Active Directory Domain Service

۲,۴ محدودسازی عضویت گروه DHCP

به منظور کنترل دسترسی به سرورهای DHCP می‌توان عضویتگروه امنیتی[۵] را روی سرور پیکربندی نمود.

- DHCP Administrator

اعضای این گروه حق دسترسی administrator به سرور را دارند (این سطح از دسترسی کمی محدودتر از سطح دسترسی Admin است). به این عمل در واقع اعمال اصل حداقل دسترسی گویند. برای پیکربندی و تخصیص میزان و نحوه دسترسی در این گروه باید از group policy استفاده کرد.

- DHCP Users

کاربران این گروه تنها حق دسترسی Read only به اطلاعات را از طریق کنسول مدیریتی DHCP دارند[۶].

۲,۵ فعال سازی Audit logging

به منظور تهیه گزارش، بررسی، ثبت وقایع و تحلیل آن‌چه برای سرور رخ می‌دهد، می‌توان از فعال سازی Audit logging استفاده نمود. این قابلیت خصوصا پس از رخدادهای کامپیوتری و برای گروه های فارنزیک بسیار مفید می‌باشد و منجر به آگاهی مدیران سیستم نسبت آنچه رخ داده، می‌گردد. علاوه بر این تغییر مکان پیش فرض لاگ ها برای عدم پاک کردن آنها توسط مهاجم یا فعال کردن تنظیمات بیشتر برای لاگ‌ها و یا حتی تغییر نام منظم لاگ‌ها می‌تواند خطر تهدیدات احتمالی از سوی مهاجمین را کاهش دهد.

---

[۵] Security Group Membership

[۶] -DHCP Administration Microsoft Management Console (MMC)

برای مثال در مورد ویندوز سرور پس از فعال‌سازی Audit Logging، در فایل C:WINNTSystem32dhcp می‌توان log های مربوطه را مشاهده کرد.

۲,۶ افزودن محدوده DHCP Reservation و Exclusion برای آدرس‌های IP

با اقدامات زیر می‌توان اطمینان حاصل کرد که به سیستم ها، آدرس IP معتبر اختصاص داده شده است.

اختصاص آدرس‌های IP به صورت استاتیک، به طوری که در دفعات بعد نیز همان آدرس به ابزار اختصاص داده شود.. در واقع بایستی آدرس IP هر ابزار در شبکه مشخص بوده و قابل انتقال به سایر ابزارهای شبکه نباشد.

- برای تمامی سیستم‌ها و ابزارهای شبکه یک محدوده خاص آدرسIP در نظر گرفته شده باشد، که هیچ سیستمی در شبکه نتواند آدرسی خارج از این محدوده داشته باشد.

۲,۷ استفاده از NAP به منظور تامین سلامت پیکربندی سیستم ها

اجرای DHCP همراه با NAP، نیازمند سیستمی است که پیش از اختصاص آدرس IP به سیستم‌های درون شبکه، بررسی سلامت آن‌ها را تایید کند. اگر بررسی سلامت سیستمی تایید نشود، آدرس IP به آن اختصاص داده خواهد شد که تنها حق دسترسی به شبکه قرنطینه شده را داشته باشد. اجرای DHCP همراه با NAP، سیستم‌های درون شبکه را وادار می‌کند هر بار که می‌خواهند، آدرس IP جدیدی داشته باشند از نظر سلامت سیستمی، بررسی شوند.

۲,۸ بستن پورت های غیر ضروری

امن سازی DHCP Server

به منظور جلوگیری از تهدیدات احتمالی توصیه میشود تمامی پورت هایی که در تبادلات ترافیمی مورد نیاز نیستند توسط مدیر سرور بسته شوند. چرا که باز بودن پورت ها می تواند مورد سوء استفاده مهاجمین قرار گیرد.

۳. چک لیست

در ادامه چک لیست متناظر برای امن سازی سرویس DHCP ارائه شده است:

ردیف	عنوان فعالیت	وضعیت
۱.	تخصیص یک کامپیوتر مجزا جهت اجرای نقش سرور DHCP	بلی/خیر
۲.	نصب windows server 2008 core (درصورت امکان)- ضمیمه بخش ۵,۱	بلی/خیر
۳.	حذف سیستم های Rogue DHCP- ضمیمه بخش ۵,۲	بلی/خیر
۴.	محدودسازی عضویت گروه[1] DHCP -ضمیمه بخش ۵,۳	بلی/خیر
۵.	افزودن محدوده DHCP Reservation و Exclusion برای آدرس های IP.	بلی/خیر
۶.	فعال سازی Audit logging	بلی/خیر
۷.	استفاده از NAP به منظور تامین سلامت پیکربندی سیستم ها	بلی/خیر
۸.	بستن پورت هایی که مورد نیاز نیستند	بلی/خیر
۹.	به روزرسانی وصله‌های نرم افزاری روی سرور DHCP	بلی/خیر

[1] Group Membership

۴. منابع

1. Windows server 2008 security guide- September 2011, available online on: activedirectory.ncsu.edu/wp-content/uploads/2011/02/windows_server_2008_R2_Security_Guide.doc
2. http://technet.microsoft.com/en-us/library/cc780347.aspx

۵. ضمیمه

۵,۱تنظیمات مربوط به core installation

از دستورات زیر می‌توان برای مدیریت سرور DHCP از طریق خط فرمان استفاده کرد.

- نصب سرور DHCP

```
start /w ocsetup DHCPServerCore
```

- پیکربندی سرور DHCP

```
sc config dhcpserver start = auto
```

- اجرای سرویس DHCP

```
net start dhcpserver
```

- پیکربندی سرور DHCP، پیکربندی حوزه های[۲] سرور DHCP و گزینه های آن:

```
netsh DHCP

netsh DHCP server

netsh DHCP server scope

netsh DHCP server mscope
```

- حذف برنامه سرور DHCP

```
start /w ocsetup DHCPServerCore /uninstall
```

۵,۲ اعمال برخی تنظیمات مربوط به حذف سیستم های DHCP Rogue

---

[۲] - Scopes

به منظور تشخیص بهتر سیستم های Rogue DHCP، می‌توان از ابزار DHCPLoc استفاده کرد. این ابزار فهرست تمامی سرورهای DHCP روی زیر شبکه محلی را نشان می‌دهد. این ابزار از بخش Support Tools در پوشه Support\Tools\ روی CD انواع ویندوز قابل دسترسی است.

۵,۳ اعمال برخی تنظیمات مربوط به محدودسازی عضویت گروه DHCP

در این بخش تنظیمات مربوط به group policy آورده شده است. از این تنظیمات می‌توان جهت اجرای پیکربندی مناسب برای هر شبکه استفاده نمود. این تنظیمات از طریق مسیر زیر اعمال می‌شوند:

Computer Configuration\Windows Settings\Security Settings\Restricted Groups

مورد سیاست	توصیف	مقدار پیش فرض
DHCP Administrators	در صورت نیاز، حساب کاربری administrator در این بخش[1] اضافه می‌شود. در صورت اضافه نمودن حساب کاربری مشابه، به طور خودکار حذف می‌شود.	Not created.
کاربران DHCP	در صورت نیاز، حساب کاربری این گروه در این بخش[2] اضافه می‌شود. در صورت اضافه نمودن حساب کاربری مشابه، به طور خودکار حذف می‌شود.	Not created.

جدول 1 - جدول group policy مربوط به سرور DHCP

[1] منظور این است که در بخش Restricted Groups ، سیاست DHCP Administrators انتخاب شود و حساب کاربری مورد نظر به آن اضافه گردد.
[2] منظور این است که در بخش Restricted Groups ، سیاست DHCP Users انتخاب شود و حساب کاربری مورد نظر به آن اضافه گردد.