بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

امن سازی سیستم عامل

گروه زیر ساخت امن

تیرماه ۱۳۹۳

فهرست مطالب

۱ مقدمه

هدف از نگارش این سند توضیح چگونگی امن‌سازی سیستم‌عامل‌های ویندوزی و لینوکسی می‌باشد. این مستند شامل غیرفعال کردن کارکردها و انجام تنظیمات پیکربندی به گونه‌ای‌ست که سیستم عامل تنها برای همان نیازهای کاربردی دلخواه کار کرده و هم چنین نقاط دسترسی[1] قابل استفاده توسط مهاجمین کمتر شده و یا در صورت امکان از بین بروند. ساختار کلی این سند بدین شکل است که ابتدا تهدیدات سیستم عامل‌ها معرفی شده، سپس دامنه و اصطلاحات به کار رفته در این سند توضیح داده می‌شود. در بخش دوم چگونگی امن‌سازی سیستم‌عامل‌ها مورد بررسی قرار گرفته، در بخش سوم این امن‌سازی به صورت چک لیست آورده می‌شود و نهایتا اطلاعات جزئی در بخش ضمیمه قابل دسترسی خواهد بود.

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 تهدیدات

از مهم‌ترین تهدیدات مرتبط به سیستم‌های عامل می‌توان به موارد زیر اشاره کرد:

[1] Access point

اسب تراوا[2]: برنامه‌ای است که به صورت پنهانی برخی فعالیت‌های مخرب را درکنار عملکرد قانونی و از پیش تعریف شده، انجام می‌دهد. برخی از اسب‌های تراوا به صورت عمدی نوشته شده‌اند و برخی دیگر نتیجه برنامه‌های قانونی هستند که به ویروس آلوده شده‌اند.

سرریز بافر و پشته[3]: این روش بسیار سنتی حمله، از باگ‌های موجود در کد سیستم به گونه‌ای استفاده می‌کند که باعث سرریز بافر می‌شود. سرریز بافر به گونه‌ای عمل می‌کند که آدرس برگشت با مقدار جدیدی پر شود و برنامه به جای برگشت به آدرس قبلی، به آدرس جدید که حاوی کد مخرب است ارجاع یابد.

پویش پورت[4]: پویش کردن پورت از مشهورترین تکنیک‌های شناسایی[5] است که مهاجمین از آن برای جستجوی پورت‌های باز سیستم استفاده می‌کنند. بدین ترتیب که پیامی به پورت‌های مختلف (معمولاً در هر لحظه به یک پورت) فرستاده می‌شود که اگر پاسخ داده شود مبنی بر فعال بودن آن پورت است. این اطلاعات در مراحل بعد جهت حمله به سیستم مورد استفاده قرار می‌گیرد.

حمله DOS: حمله DOS در واقع تلاشی برای دسترسی یا تخریب سیستم‌ها نمی‌کند، بلکه طوری آن‌ها را مسدود می‌کند که نتوانند برای هیچ کار مفیدی مورد استفاده قرار بگیرند. حلقه‌های بسته‌ای که به طور تکراری از سیستم درخواست سرویس می‌کنند نوع واضحی از این حملات هستند. سیستم‌های امنیتی که حساب کاربری را پس از تعداد مشخصی لاگین ناموفق قفل می‌کنند نیز نمود دیگری از این حمله هستند. بدین شکل که به تمامی حساب‌های کاربری به طور متعدد با رمز اشتباه لاگین می‌شود و همین امر باعث قفل شدن تمامی حساب‌ها خواهد شد.

علاوه بر تهدیدات فوق، تهدیدات زیاد دیگری وجود دارند که خارج از دامنه این مستند هستند. مهمترین علت بالا رفتن سطح این گونه تهدیدات، عدم امن سازی سیستم عامل و یا به صورت دقیق‌تر عدم اعمال تنظیمات امنیتی

---

[2] Trojan horse

[3] Stack overflow

[4] Port scan

[5] Reconnaissance

مناسب می‌باشد. به همین منظور امروزه امن سازی سیستم عامل و اعمال تنظیمات امنیتی مناسب برای سازمان یک الزام است.

۲,۱ دامنه

سند امن سازی جاری برای دو سیستم‌عامل Debian 6 و windows server 2008R2 قابل بکارگیری است. البته با تغییراتی جزئی در پیاده سازی، می‌توان از این سند برای توزیع‌های دیگر لینوکس از جمله Ubuntu و نسخه‌های دیگر ویندوز سرور استفاده کرد.

۳,۱ اصطلاحات

حمله bruteforce

رویکرد معمول در کرک پسورد، استفاده از حمله brute force است. در این حمله، مهاجم بدون هیچ گونه دانش از پسورد، تمامی پسوردهای ممکن را امتحان می‌کند تا به مقدار درست آن برسد. در بدترین حالت، مهاجم باید تمامی فضای حالت را جستجو کند.

Named pipe

در برنامه نویسی، named pipe توسعه یافته مفهوم pipe است که روشی برای انتقال اطلاعات بین پروسه‌ها می‌باشد. تفاوت آن با unnamed pipe یا همان pipe معمولی در زمان ماندگاری آن است. مفهوم Named pipe فرای لیست پروسه‌ها ایجاد می‌شود و ماندگاری سیستمی دارد، یعنی با اتمام پروسه‌ها هم چنان وجود دارد؛ اما pipe معمولی با اتمام پروسه از سیستم حذف می‌شود.

پروتکل SMB

در شبکه کامپیوتری، SMB یک نسخه از سیستم فایل اینترنتی مشترک است که به عنوان پروتکل لایه کاربرد شبکه عمل می‌کند و معمولا برای دسترسی مشترک به فایل‌ها، پرینتر و پورت‌های سریال استفاده می‌شود. این پروتکل می‌تواند بر روی لایه جلسه و یا لایه‌های پایین‌تر شبکه نیز بنشیند:

- به طور مستقیم بر روی TCP پورت ۴۴۵
- از طریق NetBIOS API روی پورت ۱۳۷و ۱۳۸ UDP و یا ۱۳۷ و ۱۳۹ TCP

SAM

مدیر حساب کاربری امنیتی[6] یا همان SAM پایگاه داده‌ای روی ویندوز سرور است که شامل حساب‌های کاربری و توصیف‌کننده‌های امنیتی برای آن‌ها می‌باشد.

[6] Security account manager

Shadow password

در حالت سنتی، فرم رمز شده پسوردها در فایل /etc/passwd با دسترسی خواندنی جهانی ذخیره می‌شود. یک برنامه برای تست یک پسورد، کافیست فرم رمز شده پسوردهای حدس زده شده را با مقادیر داخل این فایل مقایسه کند و در صورت برابری، پسورد را به دست آورد. برای جلوگیری از چنین آسیب‌پذیری، سیستم‌های جدید یونیکس از فایل‌های پسورد shadow استفاده می‌کنند که پسوردهای رمز شده را همراه با اطلاعات انقضا، در فایل /etc/shadow با دسترسی خواندنی و استفاده، تنها برای کاربر root فراهم می‌کند. دسترسی به این فایل برای سایر پروسه‌ها میبایست با مالکیت Root انجام شود.

Tcp wrapper

یک tcp wrapper کتابخانه‌ای است که کنترل دسترسی ساده‌ای را برای برنامه‌های کاربردی که اتصالات تحت شبکه را میپذیرند فراهم می‌کند. یا به عبارت دیگر، یک tcp wrapper سیستم لیست کنترل دسترسی (ACL) شبکه مبتنی بر میزبان است که برای فیلتر کردن دسترسی شبکه به اینترنت به کار می‌رود.

Syn flood

syn flood نوعی از حمله DoS است. زمانی می‌گوییم یک میزبان قربانی حمله syn flood شده است که مهاجم تلاش کند تعداد زیادی اتصال در حالت syn received ایجاد کند تا صف آن را دچار سرریز کند. حالت syn received زمانی ایجاد می‌شود که میزبان قربانی درخواست اتصال را دریافت کند و برای آن، منابع حافظه تخصیص دهد. حمله syn flood تعداد زیادی اتصال نیمه باز ایجاد می‌کند تا سیستم دیگر قادر به پاسخگویی به درخواست‌های جدید نباشد.

سرویس RPC

سرویس RPC فراخوانی روال از راه دور، پروتکلی است که به برنامه‌ها اجازه می‌دهد سرویس‌های دیگر برنامه‌ها را روی کامپیوترهای مختلف درخواست کنند. سرویس portmap سرویس‌های RPC را از طریق نگاشت شماره برنامه‌های RPC به شماره پورت‌های پروتکل DARPA کنترل می‌کند. بنابراین برای استفاده از RPC بایستی در حال اجرا باشد.

Chroot کردن

دستور Chroot یکی از قدرتمندترین امکانات محدود کردن پروسه، کاربر و یا سرویس است. این تکنیک یا به عبارت دیگر زندانی کردن یک پروسه به معنی ساختن یک دایرکتوری جایگزین برای دایرکتوری root و انتقال همه فایل‌های باینری درون آن، و اجرا کردن صحیح پروسه در محیط جدید است. پروسه (و همه‌ی پروسه‌های فرزند) باید فقط به ساختار دایرکتوری جدید دسترسی داشته باشند.

حملات ARP

پروتکل ARP برای پیوند آدرس IP و MAC مورد استفاده قرار می‌گیرد. حال آن که حملات ARP باعث می‌شوند سیستم شما فکر کند دارنده IP مثلا سیستم B همان آدرس MAC نفوذی است و هر بسته‌ای که قصد دارید سمت IP سیستم B برود به نفوذی فرستاده می‌شود.

بیت Sticky

این بیت مشخص کننده یک نوع خاص از مجوز به فایل است که وقتی بیت اصطلاحا sticky ست می‌شود، تنها مالک فایل حق حذف فایل از آن دایرکتوری را دارد. بدون بیت sticky هر کاربری که حق نوشتن دارد حق حذف فایل را نیز دارد. تنظیم sticky مانع از حذف فایل‌ها توسط کاربران دیگر می‌شود.

مجوز world-writable

هر فایل در سیستم عامل لینوکس دارای سه نوع مجوز خواندن، نوشتن و اجرا است. این مجوزها برای سه دسته کاربر مختلف تعریف می‌شوند که شامل کاربر مالک فایل، گروه مالک فایل و دیگران می‌شود. اگر مجوز فایل طوری تنظیم شده باشد که دیگران اجازه نوشتن فایل را داشته باشند به آن مجوز world-writable گوییم.

مجوز SetUID/SetGID

وقتی مجوز setuid به یک فایل داده می‌شود، پروسه‌ای که این فایل را اجرا می‌کند به جای داشتن حق دسترسی کاربر اجرا کننده، دسترسی ممتاز مبتنی بر مالک فایل پیدا می‌کند. این مجوز ویژه به کاربر اجازه دسترسی به

فایل‌ها و دایرکتوری‌هایی را می‌دهد که به طور معمولی برای مالک قابل دسترس است. به طور مثال، مجوز Setuid روی فایل passwd امکان تغییر پسوردها را برای کاربر فراهم می‌کند. مجوز Setgid نیز شبیه setuid است با این تفاوت که ID گروه موثر پروسه به گروه مالک تغییر می‌کند و امتیاز کاربر، مبنی بر امتیاز گروه بالا می‌رود.

۲ امن‌سازی

همان طور که در قسمت مقدمه اشاره شد، برای کاهش آسیب‌پذیری سیستم‌عامل در برابر تهدیدات موجود، فرآیندی به نام امن‌سازی انجام می‌شود. این فرآیند عموماً شامل مراحل قبل، حین و بعد از نصب سیستم‌عامل می‌باشد و به طور کلی شامل پیکربندی سیستم، تنظیم مجوز سیستم فایل‌ها و دایرکتوری‌ها، تنظیمات مربوط به پارتیشن‌بندی، به‌روز رسانی سیستم با استفاده از وصله‌های موجود، کنترل دسترسی، مدیریت حساب‌های کاربری، تنظیمات مربوط به جمع‌آوری و کنترل دسترسی لاگ فایل‌ها، کمینه کردن نرم‌افزارهای نصب شده و سرویس‌های در حال اجرا، امن‌سازی پشته TCP/IP و استفاده از نسخه‌های امن سرویس‌ها می‌باشد. در ادامه به طور مفصل به توضیح هر یک می‌پردازیم.

۱- **مراحل قبل نصب:** اگر مهاجم به سیستم دسترسی فیزیکی داشته باشد، می‌تواند با بوت کردن آن با سی‌دی live، به کل فضای دیسک دسترسی خواندن/نوشتن داشته باشد و هر گونه بدافزار و فایل مخرب را به سیستم تزریق کند. در این مرحله برای ممانعت از این قبیل فعالیت‌ها، دسترسی به سیستم‌عامل را محدود خواهیم کرد. این محدودیت شامل کنترل دسترسی فیزیکی سیستم (قرار دادن سیستم در جای امن)، انتخاب پسورد محکم برای Bios، تنظیم ترتیب بوت شدن سیستم و برداشتن گزینه بوت شدن از هر گونه دستگاه جانبی مانند CD Rom و USB و عدم اتصال به اینترنت قبل از نصب کامل سیستم می‌باشد.

۲- **مراحل هنگام نصب:** در این مرحله لازم است تنظیمات پارتیشن‌بندی و انتخاب سیستم فایل صحیح و مناسب انجام شود. برای پارتیشن‌بندی باید فایل‌های مربوط به سیستم‌عامل در یک پارتیشن جدا نصب شده و این پارتیشن دارای فضای کافی باشد. لاگ‌های مربوط به برنامه‌ها و سرویس‌های کاربردی نیز نباید در این پارتیشن اضافه شوند. برای انتخاب سیستم فایل مناسب و امن در مثلاً سیستم لینوکسی معمولاً توصیه می‌شود که ext3 یا ext4 استفاده شود، چرا که در این نوع سیستم فایل‌ها، هنگامی که سیستم مثلاً در اثر یک مشکل سخت افزاری crash کند

داده‌های بسیار کمی از دست خواهند رفت. به علاوه، هنگام بازیابی داده‌های از دست رفته، اگر نوع سیستم فایل ext3 یا ext4 باشد، زمانی کمتری برای بازیابی داده‌ها مورد نیاز است.

۳- **مراحل پس از نصب:** پس از آماده شدن سیستم لازم است تنظیمات زیر انجام شوند:

a) **وصله‌های امنیتی:** پس از اتمام نصب سیستم عامل، باید تمامی وصله‌های امنیتی نصب شوند. این وصله‌ها باید یا به صورت Off-line و یا از طریق سرور داخلی مانند سرور WSUS برای سیستم های ویندوزی، به‌روز شوند. در عین حال لازم است اعلان خودکار برای وجود وصله‌های امنیتی جدید نیز فعال شوند.

b) **تنظیم سیاست‌های ممیزی:**

- اعمال سیاست‌های ممیزی برای حساب‌های مختلف: فعالیت‌های روی شبکه، دستگاه‌ها و کل سیستم برای حساب‌های مختلف می‌بایست جمع‌آوری و نگه‌داری شوند.
- تنظیم پارامترهای مربوط به انتخاب پسورد خوب: پسورد خوب، پسوردی است که به راحتی قابل حدس زدن یا شکستن نباشد. قابل شکستن بدین معنی که اگر مهاجم بدون اطلاع قبلی پسوردهای زیادی را امتحان کند، مدت زمان زیادی طول بکشد تا رمز صحیح را بیابد. پسوردی که پیچیده ولی قابل حدس زدن باشد نیز عملا بی‌فایده است. به طور مثال نام شرکت Artichaud است و انتخاب پسورد 4rt1ch4ud از نظر فنی یک رمز بد محسوب می‌شود که به راحتی توسط مهاجم قابل حدس زدن است. مهاجم برای شکستن یک رمز به ترتیب پسوردهای عمومی مثل admin را امتحان می‌کند، سپس لیستی از پسوردهای مربوط به سازمان یا کارکرد سرور را شناسایی و تولید می‌کند و در مرحله بعد از دیکشنری استفاده می‌کند و در مرحله آخر از bruteforce. بدین ترتیب لازم است برخی معیارها جهت تایید خوب بودن یک پسورد اعمال شود که شامل تعیین حداقل طول و پیچیدگی است. در عین حال برای امنیت بیشتر لازم است زمان منقضی شدن پسوردها نیز تنظیم شود.
- تنظیم دقیق سطح دسترسی‌ها: لازم است دسترسی به یک سیستم و سرویس‌های در حال اجرای آن به درستی تنظیم شوند تا کاربرانی که حق دسترسی تحت شبکه دارند و نیز سرویس‌های مجاز قابل استفاده از راه دور، مشخص شوند. به طور مثال، در سیستم عامل لینوکس با استفاده از ابزار tcpwrapper می‌توان کنترل دسترسی را به سادگی برای سرویس‌ها،

کاربران و دامنه‌های مختلف تعریف کرد و یا با تکنیک Chroot پروسه‌ها و سرویس‌ها را محدود کرد.

- تنظیم پارامترهای لازم برای ثبت وقایع و لاگ‌ها: فایل‌های لاگ در شناسایی حملات در حال انجام، ارزش بسیاری دارند به همین جهت لازم است تنظیمات ثبت، تغییر مکان ذخیره‌سازی پیش فرض و تعریف سایز مناسب برای آن‌ها انجام شود و سطوح دسترسی به آن‌ها نیز مشخص گردد تا به راحتی قابل تغییر و حذف توسط کاربران نباشد.
- بررسی دوره‌ای مجوزهای اعطا شده و ویرایش آنها در صورت لزوم

c) تنظیمات امنیتی

- تنظیم بنر سازمان برای صفحه لاگین کاربران: این کار جهت مخفی کردن اطلاعات پیش فرض مورد نمایش در صفحه لاگین است مانند نسخه سیستم عامل مورد استفاده، تا مانع هر گونه سو استفاده احتمالی از این اطلاعات شود. در عین حال می‌توان برای هرگونه اتصال به سیستم یک بنر هشداردهنده در نظر گرفت که شامل اطلاعاتی است که برای شخص برقرار کننده اتصال نمایش داده می‌شود.
- ذخیره hash مربوط به پسوردها به صورت امن: پسوردهای کاربران در سیستم عامل به صورت درهم‌سازی شده ذخیره می‌شود تا از دسترسی مستقیم به پسورد واضح جلوگیری شود. جهت تامین امنیت این اطلاعات، لازم است نوع ذخیره‌سازی آن‌ها به صورت امن انجام شود تا به راحتی قابل شکستن نباشد. به طور مثال در سیستم عامل ویندوز مدل LM نوع ضعیفی از ایجاد هش است و لازم است به NTLM2 تغییر کند.
- غیر فعال کردن ارسال پسورد رمز نشده برای اتصال به یک سرور دیگر از طریق پروتکل SMB یا Samba
- محدود کردن قابلیت‌های anonymous user شامل درخواست و یا مشاهده برخی اطلاعات حساس
- فعال سازی تنظیمات امنیتی کانال داده امن برای اعضای دامنه: هنگامی که یک سیستم به یک دامنه ملحق می‌شود، یک حساب کاربری برایش ساخته می‌شود که با پسورد همان حساب،

اقدام به ایجاد یک کانال امن با کنترل کننده دامنه می‌کند. لازم است امنیت این کانال با پارامترهایی تنظیم شود.

d) تنظیمات حفاظتی:

- حذف سرویس‌ها و حساب‌های کاربری بلا استفاده از سیستم: کمینه کردن سرویس‌ها و حذف حساب‌های کاربری بلا استفاده به طور طبیعی سطح آسیب‌پذیری سیستم را کاهش می‌دهد.
- تنظیمات لازم برای امن‌سازی سرویس‌ها: پس از حذف سرویس‌های اضافه بر روی سیستم، لازم است تنظیمات امن‌سازی برای سرویس‌های باقی مانده اعمال شود. به عنوان گام اول لازم است سرویس‌های امن را جایگزین غیر امن کرد. سرویس‌هایی مانند telnet، Ftp، NIS، RPC باید حذف شده و از نسخه امن SSL آن‌ها استفاده کرد. در گام بعد باید دسترسی آن‌ها محدود شود که این کار در هر سرویس به گونه‌ای متفاوت اعمال می‌شود.
- تنظیم دقیق مجوز فایل سیستم‌ها و سطح دسترسی کاربران به آن‌ها: مجوز فایل‌ها و دایرکتوری‌های یک سیستم بسته به کاربردشان باید به درستی تنظیم شود و دسترسی کاربرانی که لازم نیست از آن‌ها حذف شود. به طور مثال، دایرکتوری home کاربران شامل تعداد زیادی فایل پیکربندی است که رفتار حساب کاربری را تحت تاثیر قرار می‌دهند. مجوز دایرکتوری home هر کاربر صرفا باید متعلق به خودش باشد. به عنوان مثال دیگر، هر فایل در سیستم عامل لینوکس دارای یک مالک است و چنان چه یک فایل بدون مالک باشد نشانه‌ای از بروز مشکل در پروسه‌های سیستم است. این امر ممکن است توسط یک نفوذی انجام شده باشد و یا به علت نصب یا حذف نادرست و یا ناکامل نرم‌افزار اتفاق افتاده باشد. چنین فایل‌هایی باید از سیستم حذف شوند. نمونه دیگر برنامه‌هایی هستند که دارای مجوز SetUID یا SetGID باشند چرا که هر باگی در این برنامه‌ها تاثیر امنیتی دارد و به حمله‌گری که خود قبلا به سیستم دسترسی داشته است اجازه می‌دهد امتیازش را افزایش دهد و کنترل خود را روی سیستم بالا ببرد. از این رو میبایست این مجوزها نیز در صورت عدم نیاز لغو شود.
- نصب و به روزرسانی آنتی ویروس.
- محدود کردن ترافیک ورودی و خروجی سیستم: لازم است، ابتدا سرویس‌ها و پورت‌های مورد نیاز در هر سرور، سرویس‌ها و پورت‌هایی با دسترسی محدود و ماشین‌هایی که از دسترسی

محدود بهره‌مند می‌شوند مورد شناسایی قرار بگیرند. سپس طبق شناسایی و نیازمندی، تنظیمات انجام شود و آزمایش شود.

- استفاده از سیاست سهمیه‌بندی[7] جهت جلوگیری از پر شدن هارد دیسک‌ها: سیستم سهمیه‌بندی مقدار فضای استفاده شده توسط کاربر را محدود به مقداری از پیش تعیین شده می‌کند. لازم است در نظر داشته باشید که سهم‌ها را به اندازه‌ای کوچک انتخاب کنید که کاربران فضای دیسک را پر نکنند، در عین حال به اندازه کافی بزرگ باشد که کاربران بابت فضای کم معترض نشوند.
- محدود کردن کاربران معمولی به دسترسی به اطلاعات روی حافظه: فایل dump، یک image از حافظه برنامه قابل اجرا است که ممکن است حاوی اطلاعات حساس باشد. در عین حال pagefile حافظه مجازی نیز ممکن است شامل اطلاعات حساس از حافظه پروسه باشد که به pagefile منتقل شده است. بنابراین لازم است ایجاد فایل Dump از حافظه یا دسترسی به محتویات pagefile مدیریت شود.
- حذف منابع به اشتراک گذاشته در صورت عدم نیاز

e) گام‌های اضافی

- هماهنگ‌سازی تاریخ و زمان در صورت وجود Time Server: زمانی که سیستم به طور غیر معمول کار کند و دچار هرگونه مشکل امنیتی شود، بررسی فایل‌های لاگ و هرگونه رد ممیزی از اهمیت خاصی برخوردار می‌شود. در بررسی این شواهد، فاکتور زمان نقش تعیین کننده‌ای دارد که اگر به اشتباه تنظیم شده باشد درستی شواهد زیر سوال خواهد رفت. بنابراین لازم است از تنظیم بودن صحیح زمان و تاریخ سیستم اطمینان حاصل شود.
- خروج حساب کاربری از سیستم پس از مدت مشخصی بیکار ماندن: لازم است screen saver برای هنگامی که کاربر کنسول را ترک می‌کند، با زمان مناسب و محدود و درخواست پسورد تنظیم شود.

---

[7] Quota

- نگهداری نسخه پشتیبان از داده‌های پایگاه داده به صورت امن: در صورتی که پایگاه داده‌ای از اطلاعات روی سیستم موجود است، لازم است به طور مرتب از داده‌های آن پشتیبان گرفته شود تا در صورت از بین رفتن اطلاعات به هر دلیلی، بتوان نزدیک‌ترین نسخه را بازیابی کرد.
- نصب نرم افزارهایی مانند HIDS برای کنترل عدم نقض تنظیمات امنیتی گفته شده مانند خاموش کردن دیواره آتش، نظارت بر صحت فایل‌های مهم، نظارت بر کاربران، نظارت بر سرویس‌ها، نظارت بر رجیستری، نظارت بر پورت‌ها و بررسی اتصال USB به سیستم
- محکم سازی پشته TCP/IP: حالت پیش فرض پیکربندی پشته TCP/IP برای کار در ترافیک اینترانت تنظیم شده است و لازم است برای کار در محیط اینترنت تغییراتی در آن ایجاد شود. این تغییرات برای جلوگیری از حملات ICMP Attack، SNMP Attack و SYN Attack می‌باشد.

۳ چک لیست

در این بخش به ارائه دو چک لیست امن سازی ویندوز سرور و لینوکس خواهیم پرداخت. لازم به ذکر است که هر ردیف چک لیست که نیاز به توضیحات اضافه داشته است در قسمت ضمیمه، دقیقا با همان شماره ردیف به آن اشاره شده است.

در ادامه چک لیست مربوط به سیستم عامل ویندوز سرور را می‌بینید:

مشخصات سرور:

نام سرور	
شماره دارایی	
آدرس IP	
آدرس MAC	
نام مدیر سرور	
تاریخ	

ردیف	عنوان فعالیت	وضعیت
۱-	**نصب و آماده‌سازی**	
۱-۱	محدودیت دسترسی فیزیکی به سیستم	بله ☐ خیر ☐
۱-۲	عدم اتصال سیستم به شبکه در حین نصب سیستم عامل جدید	بله ☐ خیر ☐
۱-۳	ایجاد پسورد برای BIOS (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۱-۴	تنظیم ترتیب بوت شدن سیستم (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-	**وصله‌های امنیتی**	
۲-۱	نصب تمامی وصله‌های امنیتی پس از اتمام نصب سیستم عامل	بله ☐ خیر ☐
۲-۲	فعال سازی اعلان خودکار برای وجود وصله‌های امنیتی جدید (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-	**تنظیم سیاست‌های ممیزی**	
۳-۱	تنظیم سیاست‌های ممیزی برای حساب‌های مختلف (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲	تعیین حداقل طول پسورد**.Error! Reference source not found.** (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳	فعال‌سازی فیلدهای پیچیدگی پسورد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴	تعیین زمان انقضای پسورد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۵	تنظیم پارامترهای لازم برای ثبت وقایع و لاگ‌ها (به بخش ۴ رجوع شود)	بله ☐ خیز ☐
۴-	**تنظیمات امنیتی**	
۴-۱	غیر فعال کردن درخواست شناسه امنیتی کاربران دیگر توسط کاربر anonymous (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۲	عدم اجازه برای شمارش کاربران موجود در SAM توسط کاربر anonymous (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۳	عدم اجازه برای شمارش فایل‌های به اشتراک گذاشته در شبکه توسط کاربر anonymous (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۴	غیر فعال کردن کاربر Guest (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۵	فعال سازی تنظیمات امنیتی کانال داده امن هنگام اضافه شدن یک سیستم به عنوان عضوی از دامنه (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۶	قرار دادن banner سازمان در محل لاگین کاربران (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۷	غیر فعال کردن ارسال پسورد رمز نشده برای اتصال به یک سرور دیگر از طریق SMB (به	بله ☐ خیر ☐

	بخش ۴ رجوع شود)	
۸-۴	عدم اجازه به هر کاربر برای استفاده از کاربر anonymous (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۹-۴	عدم اجازه در استفاده از named pipeها به کاربر anonymous (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۱۰-۴	حصول اطمینان از اینکه هیچ فایل یا پوشه‌ی اشتراکی از طریق کاربر anonymous قابل دسترسی نمی‌باشد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۱۱-۴	عدم ذخیره سازی هش ضعیف Lan manager از پسورد در مواقع تغییر آن (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۱۲-۴	تنظیم سطح LAN Manager Authentication به NTLMv2 (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۱۳-۴	تنظیم لاگین تحت شبکه حساب‌های کاربری محلی به گونه‌ای که با همان حساب‌های کاربری خودشان احراز هویت شوند (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۵-	**تنظیمات حفاظتی**	
۱-۵	حذف سرویس‌های بدون استفاده (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۵	حذف حساب‌های کاربری بلا استفاده	بله ☐ خیر ☐
۳-۵	تنظیم سطح دسترسی کاربران به صورت کاملا امن (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۵	تنظیم امن مجوزهای فایل سیستم‌ها	بله ☐ خیر ☐
۵-۵	بررسی پورت‌ها و فعال سازی فایروال‌های شخصی و محدود سازی ترافیک (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۵	پیکربندی کلیدهای رجیستری پشته TCP/IP جهت محافظت در برابر حملات DoS (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-	**گام‌های اضافه**	
۱-۶	تنظیم تاریخ و زمان. در صورت وجود time server، هماهنگ شدن با آن	بله ☐ خیر ☐
۲-۶	نصب و به روز رسانی روزانه آنتی‌ویروس	بله ☐ خیر ☐
۳-۶	تنظیم screen saver و ایجاد پسورد برای هنگامی که کاربر کنسول را ترک می‌کند. (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۴-۶	اعمال سیاست سهمیه‌بندی فضای دیسک (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۵-۶	نصب نرم افزارهایی برای تست صحت فایل‌های حساس سیستم (به بخش ۴ رجوع شود)	بله ☐ خیر ☐

۶-۶	اگر از پروتکل RDP استفاده می‌شود، تنظیم سطح رمز نگاری به سطح High (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۷	عدم استفاده از نام کاربری Administrator و تغییر آن به نام دیگر (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۸	جلوگیری از اجرای Autorun درایوهای قابل حمل و cd-rom (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۹	بررسی و پاکسازی برنامه‌های مشکوکی که هنگام بارگذاری ویندوز اجرا می‌شوند. (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۰	پاک سازی PageFile در حین خاموش کردن ویندوز با شرایطی (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۱	استفاده از نرم‌افزار BitLocker برای محافظت بیشتر از داده‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۲	غیر فعال کردن AutoAdminLogon (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۳	غیرفعال کردن کش کردن logonها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۴	غیر فعال کردن AutoShareServer (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۶-۱۵	نمایش فایل‌های مخفی و فرمت فایل‌ها جهت چک کردن فایل‌های مشکوک به طور دوره‌ای (به بخش ۴ رجوع شود)	بله ☐ خیر ☐

در ادامه چک لیست مربوط به سیستم عامل Debian 6 را می‌بینید:

مشخصات سرور:

نام سرور	
شماره دارایی	
آدرس IP	
آدرس MAC	
نام مدیر سرور	
تاریخ	

ردیف	عنوان	وضعیت
۱-	**قبل نصب**	
۱-۱	محدودیت دسترسی فیزیکی به سیستم	بله ☐ خیر ☐
۱-۲	عدم اتصال سیستم به شبکه در حین نصب سیستم عامل جدید	بله ☐ خیر ☐
۱-۳	ایجاد پسورد برای BIOS و تنظیم ترتیب بوت شدن سیستم برای جلوگیری از بوت شدن از رسانه‌های جایگزین	بله ☐ خیر ☐
۲-	**حین نصب**	
۲-۱	قرار دادن پوشه‌های مهم قابل نوشتن در پارتیشن‌های جداگانه (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۲	قرار دادن نرم‌افزارهای غیرمرتبط با سیستم‌عامل در پارتیشن مجزا (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۳	قراردادن داده‌های ایستایی که نیاز به تغییر ندارند در پارتیشن مجزا با مجوز read-only	بله ☐ خیر ☐
۲-۴	عدم اتصال به اینترنت تا آماده شدن کامل سیستم (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۵	انتخاب فایل سیستم مناسب مانند ext3 یا ext4 (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۶	تنظیم پسورد محکم و قوی برای کاربر root (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۷	فعال کردن Shadow password (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۸	نصب حداقل سرویس‌ها بخصوص سرویس‌های تحت شبکه هنگام نصب سیستم‌عامل (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۲-۹	نصب حداقل نرم‌افزارها هنگام نصب سیستم‌عامل (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-	**پس از نصب**	
۳-۱	**به روز رسانی**	
۳-۱-۱	به روز رسانی وصله‌های امنیتی به صورت آفلاین و یا آنلاین پس از تنظیمات فایروال (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۱-۲	به روزرسانی کتابخانه‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۱-۳	اضافه کردن وصله‌های هسته[8] (به بخش ۴ رجوع شود)	بله ☐ خیر ☐

[8] Kernel

۳-۲	**تنظیمات سرویس‌ها**	
۳-۲-۱	امن‌سازی سرویس ssh (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۲	امن‌سازی سرویس Ftp (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۳	دسترسی امن به سیستم پنجره X (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۴	غیرفعال کردن NIS (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۵	امن‌سازی سرویس RPC (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۶	تنظیمات مربوط به فایروال براساس نیازمندی‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۷	عدم استفاده از سرویس‌هایی که از پسورد متن واضح استفاده می‌کنند (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۲-۸	chroot کردن سرویس‌های تحت شبکه (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳	**کنترل دسترسی و حساب‌های کاربری**	
۳-۳-۱	تنظیم پسورد برای Grub (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۲	محدود کردن ریبوت سیستم صرفا از طریق کنسول (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۳	محدود کردن اجازه دسترسی به cron به کاربر root (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۴	استفاده از tcpwrapper جهت کنترل دسترسی به سرویس‌ها از طریق میزبان‌ها و دامنه‌های مختلف (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۵	اطمینان از عدم وجود دایرکتوری‌های null و یا مسیرهای نسبی در PATH مربوط به root (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۶	اطمینان از عدم وجود مجوز world-writable یا group-writable در مدخل[9]های PATH مربوط به root (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۷	اطمینان از عدم قابلیت نوشتن توسط گروه و دیگران برای دایرکتوری home کاربران (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۸	اطمینان از عدم وجود مجوز world-writable در فایل‌های دات (پنهان) کاربر (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۳-۹	تنظیم پارامترهای انقضای پسورد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐

[9] Entry

۳-۳-۱۰	تنظیم پارامترهای طول و پیچیدگی پسورد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴	**تنظیمات مجوز فایل‌ها و دایرکتوری‌های مهم**	
۳-۴-۱	محدود کردن مجوز پارتیشن‌های مختلف (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۲	بررسی و تایید مجوز فایل‌های shadow، Group، gshadow و passwd (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۳	بررسی تمامی دایرکتوری‌های world-writable برای داشتن بیت‌های Sticky (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۴	یافتن فایل‌های world-writable غیر مجاز (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۵	یافتن فایل‌های بدون مالک و اصلاح آن‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۶	بررسی تمامی دایرکتوری‌های world-writable جهت صحیح بودن مالکیت آن‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۴-۷	کمینه کردن برنامه‌های SetUID/SetGID (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۵	**مدیریت حساب‌های کاربری**	
۳-۵-۱	داشتن فرم کاغذی جهت ثبت نام کاربران برای حساب کاربری. (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۵-۲	شناسایی کاربران به طور فیزیکی قبل از دادن هرگونه حساب کاربری و امتیاز.	بله ☐ خیر ☐
۳-۵-۳	غیر فعال کردن هر گونه حساب کاربری guest.	بله ☐ خیر ☐
۳-۵-۴	غیر فعال کردن هر گونه حساب بدون پسورد (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۵-۵	جستجو و حذف تمامی فایل‌های مربوط به حساب کاربری بلافاصله پس از حذف حساب کاربر	بله ☐ خیر ☐
۳-۵-۶	چک کردن این که حساب‌های کاربری حذف شده Cron نداشته باشند.	بله ☐ خیر ☐
۳-۵-۷	از بین بردن پروسه‌های در حال اجرا با شناسه UID مربوط به حساب کاربری حذف شده (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶	**دیگر موارد**	
۳-۶-۱	پیکربندی جهت ثبت و جمع‌آوری فایل‌های لاگ (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۲	انتقال داده تحت شبکه به صورت امن (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۳	اعمال سیاست سهمیه‌بندی فضای دیسک (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۴	چک کردن صحت فایل‌های سیستم (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۵	امن‌سازی دسترسی تحت شبکه (به بخش ۴ رجوع شود)	بله ☐ خیر ☐

۳-۶-۶	گرفتن Snapshot از سیستم و پشتیبان‌گیری دوره‌ای از داده‌ها و سیستم فایل (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۷	محافظت در برابر حملات ARP (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۸	تنظیم بنر هشداردهنده برای دسترسی به سیستم (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۹	محافظت با آنتی‌ویروس (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۱۰	غیر فعال کردن ipv6 در صورت عدم استفاده (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۱۱	غیر فعال کردن Core dump (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۱۲	بررسی صحت وصله‌ها و به‌روزرسانی‌ها قبل از نصب آن‌ها (به بخش ۴ رجوع شود)	بله ☐ خیر ☐
۳-۶-۱۳	نصب نرم افزارهای HIDS برای تضمین صحت فایل‌های حساس سیستم	بله ☐ خیر ☐

۴ منابع

1. www.debian.com/doc/manuals/securing-debian-howto
2. www.wikis.utexas.edu/display/ISO/Windows+2008R2+Server+Hardening+Checklist
3. www.msdn.microsoft.com/en-us/library/dd163561.aspx

۵ ضمیمه

۱،۵ امن‌سازی ویندوز سرور

چک لیست امن‌سازی ویندوز سرور با شماره آن در جدول به تفصیل در زیر شرح داده شده است.

ردیف ۱-۳: ایجاد پسورد برای BIOS

در حین روشن شدن کامپیوتر باید وارد تنظیمات bios شد. (با زدن دکمه Del) و تنظیمات مربوطه انجام شود.

ردیف ۱-۴: تنظیم ترتیب بوت شدن

ترتیب بوت شدن باید ابتدا بر روی هارد باشد تا هکرها با cdهای بوت به راحتی نتوانند سیستم را راه‌اندازی کنند.

ردیف ۲-۲: فعال‌سازی اعلان خودکار برای وجود وصله‌های امنیتی جدید

در start باید windows update جستجو شود و لینک را کلیک کرد. در پنجره باز شده لینک let me choose my settings را کلیک کرده و در پنجره باز شده نیز می‌توان یکی از دو گزینه زیر را انتخاب کرد.

Download updates for me, but let me choose when to install them.
Notify me but don't automatically download or install them

ردیف ۳-۱: تنظیم سیاست‌های ممیزی برای حساب‌های مختلف

ممیزی[10] روشی برای جمع‌آوری و نگه‌داری فعالیت‌های روی شبکه، دستگاه‌ها و کل سیستم است. برای تنظیم کردن مواردی که جمع‌آوری شود باید به صورت زیر عمل کرد:

با تایپ عبارت gpedit.msc در start وارد ویرایشگر مورد نظر شوید سپس به مسیر زیر بروید.

Computer Configuration\Windows setting\security setting\advanced audit policy\system audit policies

سپس موارد زیر را تنظیم کنید:

	گروه	زیرگروه	تنظیم	توضیحات
۱	System	IPsec Driver	Success and Failure	برای server و WS[11] و DC[12]
۲	System	Security State Change	Success and Failure	برای server و WS و DC
۳	System	Security System Extension	Success and Failure	برای server و WS و DC
۴	System	System Integrity	Success and Failure	برای server و WS و DC
۵	Logon-Logoff	Logoff	Success	برای server و WS و DC
۶	Logon-Logoff	Logon	Success Success and Failure	برای server و WS و DC

[10] Auditing

[11] Workstation

[12] Domain controller

				برای امنیت شدیدتر در سیستم‌های ویژه
۷	Logon-Logoff	Special Logon	Success	برای server و WS و DC
۸	Object Access	File System	No auditing Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۹	Object Access	Registry	No auditing Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۰	Privilege Use	Sensitive Privilege Use	No auditing Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۱	Detailed Tracking	Process Creation	Success	برای server و WS و DC
۱۲	Policy Change	Audit Policy Change	Success and Failure	برای server و WS و DC
۱۳	Policy Change	Authentication Policy Change	Success	برای server و WS و DC
۱۴	Account Management	Computer Account Management	Success Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۵	Account Management	Distribution Group Management	No auditing Success	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۶	Account Management	Other Account Management Events	Success Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۷	Account Management	Security Group Management	Success Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۸	Account Management	User Account Management	Success Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه
۱۹	Account Logon	Credential Validation	Success Success and Failure	برای server و WS و DC برای امنیت شدیدتر در سیستم‌های ویژه

۲۰	DS Access	Directory Service Access	Success Success and Failure	فقط برای DC فقط برای DC با سطح امنیتی شدید
۲۱	DS Access	Directory Service Changes	Success Success and Failure	فقط برای DC فقط برای DC با سطح امنیتی شدید

ردیف ۳-۲: تعیین حداقل طول پسورد

با تایپ عبارت Local Security Policy در start وارد کنسول مورد نظر شوید. سپس وارد پوشه‌های زیر شوید:

Account Policies > Password Policies

سپس Policy مورد نظر که Minimum password length می‌باشد را باز کرده و کمترین طول پسورد را وارد کنید.

ردیف ۳-۳: فعال‌سازی فیلدهای پیچیدگی پسورد

با تایپ عبارت Local Security Policy در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Account Policies > Password Policies

سپس Policy مورد نظر که Password must meet complexity requirements می‌باشد را باز کرده آنرا enabled کنید.

ردیف ۳-۴: تعیین زمان انقضای پسورد

با تایپ عبارت Local Security Policy در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Account Policies > Password Policies

سپس Policy مورد نظر که Maximum password age می‌باشد را باز کرده و مقدار آن را متناسب با سیاست‌های سازمان خود تغییر دهید.

ردیف ۳-۵: تنظیم پارامترهای لازم برای ثبت وقایع و لاگ‌ها

با تایپ عبارت gpedit.msc در start وارد ویرایشگر مورد نظر شوید، سپس به مسیر زیر بروید.

Computer Configuration\Administrative Templates\Windows Components\Event Log Service.

سپس برای تمامی logها، ابتدا آنها را فعال کرده و سپس تنظیمات دیگر از قبیل سایز و مکان ذخیره کردن log انجام شود.

ردیف ۴-۱: غیر فعال کردن درخواست شناسه امنیتی کاربران دیگر توسط کاربر anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Allow anonymous SID/Name translation می‌باشد را باز کرده آنرا disabled کنید.

ردیف ۴-۲: عدم اجازه برای شمارش کاربران موجود در SAM توسط کاربر anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید. سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Do not allow anonymous enumeration of SAM accounts می‌باشد را باز کرده آنرا Enabled کنید.

ردیف ۴-۳: عدم اجازه برای شمارش فایل‌های به اشتراک گذاشته در شبکه توسط کاربر anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Do not allow anonymous enumeration of SAM accounts and shares می‌باشد را باز کرده آنرا Enabled کنید.

ردیف ۴-۴: غیر فعال کردن کاربر Guest

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Accounts: Guest account status می‌باشد را باز کرده آنرا Disable کنید.

ردیف ۴-۵: فعال‌سازی تنظیمات امنیتی کانال داده امن هنگام اضافه شدن یک سیستم به عنوان عضوی از دامنه

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policyهای زیر را باز کرده آنرا Enabled کنید.

Domain member: Digitally encrypt or sign secure channel data (always)
Domain member: Digitally encrypt secure channel data (when possible)
Domain member: Digitally sign secure channel data (when possible)

ردیف ۴-۶: قرار دادن banner سازمان در محل لاگین کاربران

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که interactive logon: Message text for users attempting to log on می‌باشد را باز کرده و در داخل کادر متن مورد نظر را می‌نویسیم.

ردیف ۴-۷: غیر فعال کردن ارسال پسورد رمز نشده برای اتصال به یک سرور دیگر از طریق SMB

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Microsoft network client: Send unencrypted password to connect to third-party SMB servers می‌باشد را باز کرده و Disabled می‌کنیم.

ردیف ۴-۸: عدم اجازه به هر کاربر برای استفاده از کاربر anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Let Everyone permissions apply to anonymous users می-باشد را باز کرده و Disabled می‌کنیم.

ردیف ۴-۹: عدم اجازه برای استفاده از namedpipeها به کاربران anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Named pipes that can be accessed anonymously می‌باشد را باز کرده و Disabled می‌کنیم.

همچنین Policy مورد نظر دیگر Network access: Restrict anonymous access to Named Pipes and Shares را نیز Enabled می‌کنیم.

ردیف ۴-۱۰: حصول اطمینان از قابل دسترس نبودن هرگونه فایل یا پوشه اشتراکی از طریق کاربر anonymous

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Shares that can be accessed anonymously می‌باشد را باز کرده و اگر چیزی داخل کادر نوشته شده باشد را پاک می‌کنیم.

ردیف ۴-۱۱: عدم ذخیره سازی هش ضعیف Lan manager از پسورد در مواقع تغییر آن

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network security: Do not store LAN Manager hash value on next password change می‌باشد را باز کرده و Enabled می‌کنیم.

ردیف ۴-۱۲: تنظیم سطح Lan manager authentication به NTLMv2

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network security: LAN Manager authentication level می‌باشد را باز کرده و send NTLMv2 response only را انتخاب می‌کنیم.

ردیف ۴-۱۳: تنظیم لاگین تحت شبکه حساب‌های کاربری محلی به گونه‌ای که با همان حساب‌های کاربری خودشان احراز هویت شوند

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Network access: Sharing and security model for local accounts می‌باشد را باز کرده و classic را انتخاب می‌کنیم.

ردیف ۵-۱: حذف سرویس بدون استفاده

برای این منظور می‌توان با تایپ SCW(Security Configuration Wizard) وارد کنسول موردنظر شد. با توجه به roleهای انتخاب شده تنظیمات انجام شود !

ردیف ۵-۳: تنظیم سطح دسترسی کاربران به طور کاملا امن

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies-> User Rights Assignment

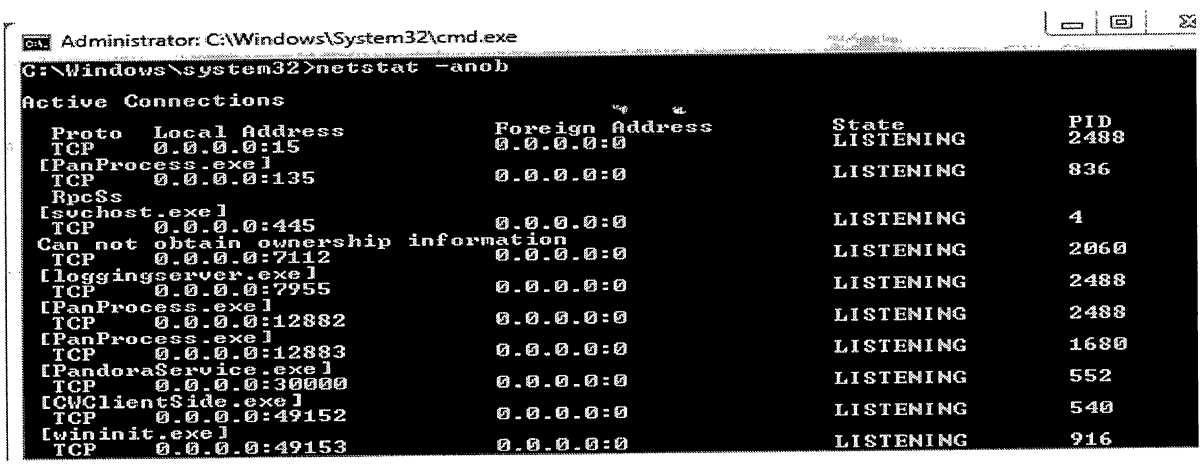
یکی از حقوق مهمی که باید محدود شود اجازه دسترسی به کامپیوتر از طریق شبکه می‌باشد. برای این منظور Access this computer from the network را باز کرده و کاربرانی که نباید اجازه دسترسی داشته باشند از لیست حذف شوند.

کاربران پیشنهادی: Administrator, Authenticated Users

ردیف ۵-۵: بررسی پورت‌ها و فعال‌سازی فایروال شخصی و محدودسازی ترافیک

ابتدا باید cmd را run as administrator اجرا کرد. سپس دستور netstat –anob را اجرا می‌کنیم. با این کار تمامی portهای باز سیستم نمایش داده می‌شود. Portهایی که برای ما مهم است که باز نباشند عبارتند از: ۱۳۵، ۱۳۹-۱۳۷، ۴۴۵.

برای بستن این پورت‌ها راه‌های مختلفی وجود دارد. اولین راه حل بستن سرویسی که از این پورت استفاده می‌کند می‌باشد. برای این منظور در شکل زیر PID بیانگر ID سرویسی می‌باشد که از port مورد نظر استفاده می‌کند.



سپس با زدن دکمه‌های Alt+Ctrl+Del به پنجره services می‌رویم. در آنجا سرویسی که PID موردنظر را دارد stop می‌کنیم.

راه دوم: block کردن port مورد نظر توسط firewall می‌باشد. برای این منظور باید به تنظیمات فایروال در کنترل پنل برویم. در آنجا وارد advance setting می‌شویم. هم برای inbound و هم outbound یک rule جدید اضافه می‌کنیم. باید بر روی آنها راست کلیک کرده و new rule را بزنیم. در آنجا Port را انتخاب می‌کنیم و به صفحه بعد می‌رویم. در بخش بعدی شماره port موردنظر را وارد می‌کنیم. در صفحه بعد گزینه block the connection را انتخاب می‌کنیم. در صفحات بعدی نام و توضیح برای rule می‌نویسیم.

بدین ترتیب ارتباط port مورد نظر با دنیای خارج قطع می‌شود. توجه شود که هم برای ترافیک ورودی و هم خروجی انجام شود.

ردیف ۵-۶: پیکربندی کلیدهای رجیستری پشته TCP/IP جهت محافظت در برابر حملات DoS

برای این کار باید برخی از کلیدهای رجیستری تغییر کنند و از آن جایی که این کار ریسک بالایی دارد، بهتر است ابتدا از کلیدهای رجیستری خود نسخه پشتیبان بگیرید و سپس تغییرات را اعمال کنید:

در run عبارت regedit را تایپ کنید و به مسیر زیر بروید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

و متغیر SynAttackProtect را به ۱، EnableDeadGWDetect به صفر، EnablePMTUDiscovery را به صفر، KeepAliveTime را ۳۰۰۰۰۰ معادل ۵ دقیقه و NoNameReleaseOnDemand را به ۱ تنظیم کنید.

ردیف ۶-۳: نصب screen saver و ایجاد پسورد برای زمانی که کاربر کنسول را ترک می‌کند.

در run عبارت screen saver را تایپ کنید. و بعد از انتخاب مدل، بر روی آن رمز نیز باید گذاشته شود.

ردیف ۶-۴: اعمال سیاست سهمیه‌بندی فضای دیسک

برای این کار کافیست در windows explorer روی هر یک از درایوهای موجود راست کلیک کرده و روی تب quotas دکمه show quota setting کلیک کنید. سپس تنظیمات مقدار فضای دیسک را انجام دهید. برای محدود کردن هر کاربر به طور جداگانه بایستی روی Quota entries کلیک کنید و تنظیمات را از آن جا انجام دهید.

ردیف ۶-۵: نصب نرم‌افزارهایی برای تست صحت فایل‌های حساس سیستم

با اجرای دستور SFC /SCANNOW در cmd می‌توان تغییر در فایل‌های سیستمی را متوجه شد. همچنین می‌توان از نرم افزارهای تشخیص نفوذ مبتنی بر هاست[۱۳] نیز جهت چک کردن صحت فایل‌ها استفاده کرد. از جمله این نرم‌افزارها می‌توان به Ossec اشاره کرد.

ردیف ۶-۶: تنظیم سطح رمزنگاری به سطح high در صورت استفاده از پروتکل RDP

---

[13] HIDS

Gpedit.msc را در start تایپ کنید. سپس به آدرس زیر بروید.

Computer Configuration-> Administrative Templates-> Windows Components-> Remote desktop service-> Security -> client connection encryption level

و سپس آنرا فعال کنید و سطح امنیتی را به High تغییر دهید. همچنین require the use of a specific security layer connections و سپس آنرا نیز فعال کنید و سطح آن را SSL (TLS 1.0) قرار دهید.

ردیف ۶-۷: تغییر نام و عدم استفاده از Administrator

ایجاد و استفاده از user دیگر با امکانات محدود به جای استفاده از administrator. – فقط در صورت نیاز از admin استفاده شود. همچنین نام administrator را تغییر دهید. برای این منظور وارد محیط group policy شوید. به آدرس زیر بروید:

Computer Configuration-> windows setting->Local Policies->Security Options

سیاست مورد نظر یعنی Accounts: Rename administrator account را باز کرده و نام administrator را تغییر دهید.

ردیف ۶-۸: جلوگیری از اجرای autorun درایوهای قابل حمل و cd-rom

برای برداشتن قابلیت autorun باید gpedit را در start تایپ کنید. سپس به آدرس زیر بروید.

Computer Configuration-> Administrative Templates-> Windows Components->autoplay policies-> turn of Autoplay

دو مورد زیر را Enable کنید.

Turn off Autoplay
Turn off Autoplay for non-volume devices

ردیف ۶-۹: بررسی و پاکسازی برنامه‌های مشکوکی که هنگام بارگذاری ویندوز اجرا می‌شوند

یکی از کارهایی که بسیاری از ویروس‌ها برای بقای خود انجام می‌دهند دستکاری رجیستری به منظور اجرای خود در حین بالا آمدن ویندوز می‌باشد. به طوریکه اگر ویندوز reset شود باز هم ویروس اجرا شود. چندین کلید

رجیستری برای تنظیم این کار وجود دارد. با بررسی این کلیدها و یافتن موارد مشکوک می‌توان از احتمال وجود ویروس مطلع شد. کلیدهای موردنظر عبارتند از:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

ردیف ۶-۱۰: پاکسازی PageFile در حین خاموش کردن ویندوز

با تایپ عبارت secpol.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Local Policies->Security Options

سپس Policy مورد نظر که Shutdown: Clear virtual memory pagefile می‌باشد را باز کرده و enable را انتخاب می‌کنیم.

لازم به ذکر است که اگر چندین سیستم عامل بر روی یک ماشین نصب شده باشد، بهتر است این گزینه را Enable کنید. زیرا PageFile یک سیستم عامل از دیگر سیستم عامل‌ها قابل خواندن است. ولی اگر تنها یک سیستم عامل بر روی یک ماشین نصب است، این PageFile قفل و غیر قایل خواندن خواهد شد. با داشتن تنها یک سیستم عامل، نباید اقدام به پاک کردن این محتویات بکنید، زیرا ممکن است در زمان تحلیل فارنزیکی مفید واقع شوند.

ردیف ۶-۱۱: استفاده از نرم‌افزار BitLocker برای محافظت بیشتر از داده‌ها

استفاده از نرم افزار رمزنگاری و امن سازی اطلاعات همچون BitLocker : رمزگذاری درایو با BitLocker که روی ویندوز سرور ۲۰۰۸ قابل دسترسی می‌باشد، همچنین این ویژگی در ویرایش‌های سطح بالاتر ویندوز ویستا و ویندوز ۷ نیز در دسترس قرار دارد. این ویژگی، امکان محافظت از کل ولوم‌های دیتا (Data Volume) غیر از ولوم سیستم عامل را با رمزنگاری فراهم می‌کند. اگر یک سیستم دزدیده شود، Bitlocker باعث می‌شود بوت نمودن آن از یک ولوم اضافی و سپس دسترسی به داده‌های موجود بسیار دشوارتر باشد. این قابلیت می‌تواند از داده‌های عادی و همچنین داده‌های سیستم عامل مانند بانک اطلاعاتی اکتیو دایرکتور روی یک کنترلر دامنه، محافظت کند .تمامی کارمندان صرف نظر از موقعیت شغلی یا نوع اطلاعاتی که روی لپ تاپ‌های شان نگهداری می‌کنند، باید این

اطلاعات را به صورت رمزنگاری شده ذخیره کنند. در صورتی که همه اطلاعات روی لپ تاپ‌ها به صورت رمزنگاری نگهداری شوند، هرگاه لپ تاپ کارمندی گم شده یا به سرقت رود، کلیه فایل‌ها، اطلاعات کاری، رمزهای عبور و تاریخچه اینترنت گردی وی دور از دسترس افراد غیر مجاز خواهند بود.

ردیف ۶-۱۲: غیرفعال کردن AutoAdminLogon

به آدرس HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon بروید و مقدار کلید موردنظر را به ۰ تغییر دهید.

ردیف ۶-۱۳: غیرفعال کردن کش کردن Logonها

با تایپ عبارت gpedit.msc در start وارد کنسول مورد نظر شوید، سپس وارد پوشه‌های زیر شوید:

Computer Configuration->Local Policies->Security Options

سپس Policy مورد نظر که Interactive logon: Number of previous logons to cache (in case domain controller is not available می‌باشد را باز کرده و مقدار آنرا ۰ قرار دهید.

ردیف ۶-۱۴: غیرفعال کردن AutoShareServer

اگر از sharingهای (C$, D$, ADMIN$) استفاده نمی‌کنید به آدرس:

HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\

بروید و یک کلید جدید از نوع DWord به نام AutoShareServer ایجاد کنید مقدار کلید موردنظر را ۰ قرار دهید.

ردیف ۶-۱۵: نمایش فایل‌های مخفی و فرمت فایل‌ها جهت چک کردن فایل‌های مشکوک به طور دوره‌ای

اکثر ویروسها برای اینکه از دید کاربر پنهان باشند خود را مخفی می‌کنند (Hidden) . آنها به خود هم صفت Hidden و هم صفت System می‌دهند، اگر تصمیم به مشاهده فایل‌های Hidden و System دارید می‌بایست در

Folder Options در تب View علاوه بر فعال کردن Show hidden files , folders and drives می‌بایست Hide protected operating system files را غیر فعال کنید همچنین با غیرفعال کردن گزینه Hide extensions for known file types می‌توانید پسوند فایلها را در ویندوز مشاهده کنید، با توجه به اینکه پسوند اکثر ویروسها exe.است (اکثریت نه همه !!!) زمانی که شما پسوند فایلها را نمایش میدهید ممکن است فایلی در فلشتان مشاهده کنید که با آیکن عکس یا فولدر و یا دیگر آیکن‌های فریب دهنده باشد ولی وقتی به پسوند آن دقت می‌کنید می‌بینید که پسوند آن exe. است و هیچ چیز شک برانگیز تر از این نخواهد بود، پس با انجام این کارها هم می‌توانید ویروسهایی که خود را از چشم کاربر مخفی می‌کنند ببینید و هم با مشاهده پسوندهای شک برانگیز متوجه ویروسی بودن سیستم شوید. توجه به این نکته ضروریست که پس از چک کردن فایل‌ها و پسوندها، بهتر است نمایش آن‌ها را به حالت قبل برگردانید تا باعث حذف و تغییر ناخواسته فایل‌های سیستمی توسط کاربر غیر حرفه‌ای نشوید.

۲,۵ امن‌سازی debian

چک لیست امن‌سازی Debian سرور با شماره آن در جدول به تفصیل در زیر آورده شده است.

ردیف ۲-۱: قرار دادن پوشه‌های مهم در پارتیشن‌های مجزا

هر پوشه ای مانند /tmp، /home، /var/log و /var/tmp کاربران مجوز نوشتن را دارند را باید در یک پارتیشن جدا قرار داد. چرا که کاربر می‌تواند با یک حمله DOS، نقطه mount مربوط به / را پر کرده و سیستم را unavailable کند. هر چند در برخی سیستم عامل‌های امروزی یک فضای محافظت شده برای جلوگیری از این حملات در نظر گرفته می‌شود.

ردیف ۲-۲: قرار دادن نرم‌افزارهای غیرمرتبط با OS در پارتیشن مجزا

هر نرم افزاری که مرتبط با سیستم عامل نصب شده نیست باید در یک پارتیشن جدا نصب شود. این نرم افزارها معمولاً در /opt و /usr/local نصب می‌شوند. چرا که اگر سیستم عامل را دوباره نصب کنیم نیاز به نصب مجدد این نرم افزارها نیست.

ردیف ۲-۴: عدم اتصال به اینترنت تا آماده شدن کامل سیستم

در حین نصب و یا بلافاصله بعد از نصب سیستم عامل، نباید سیستم را به اینترنت متصل کرد. چرا که ممکن است سیستم مورد حمله قرار گیرد. ابتدا باید سیستم عامل به صورت کامل نصب کرد سپس وصله‌های امنیتی به روز را یا از طریق یک سیستم مدیریت وصله‌ها گرفت و یا ابتدا تنظیمات مناسب فایروال را انجام داد و سپس به صورت مستقیم از اینترنت گرفت.

ردیف ۲-۵: انتخاب فایل سیستم مناسب

معمولاً توصیه می‌شود که از سیستم فایل ext3 یا ext4 استفاده شود، چرا که این نوع سیستم فایل‌ها، هنگامی که سیستم مثلاً در اثر یک مشکل سخت افزاری crash کند داده‌های بسیار کمی از دست خواهند رفت. به علاوه، هنگامی بازیابی داده‌های از دست رفته، اگر نوع سیستم فایل ext3 یا ext4 باشد، زمانی کمتری برای بازیابی داده‌ها مورد نیاز است.

ردیف ۲-۶: تنظیم پسورد محکم برای root

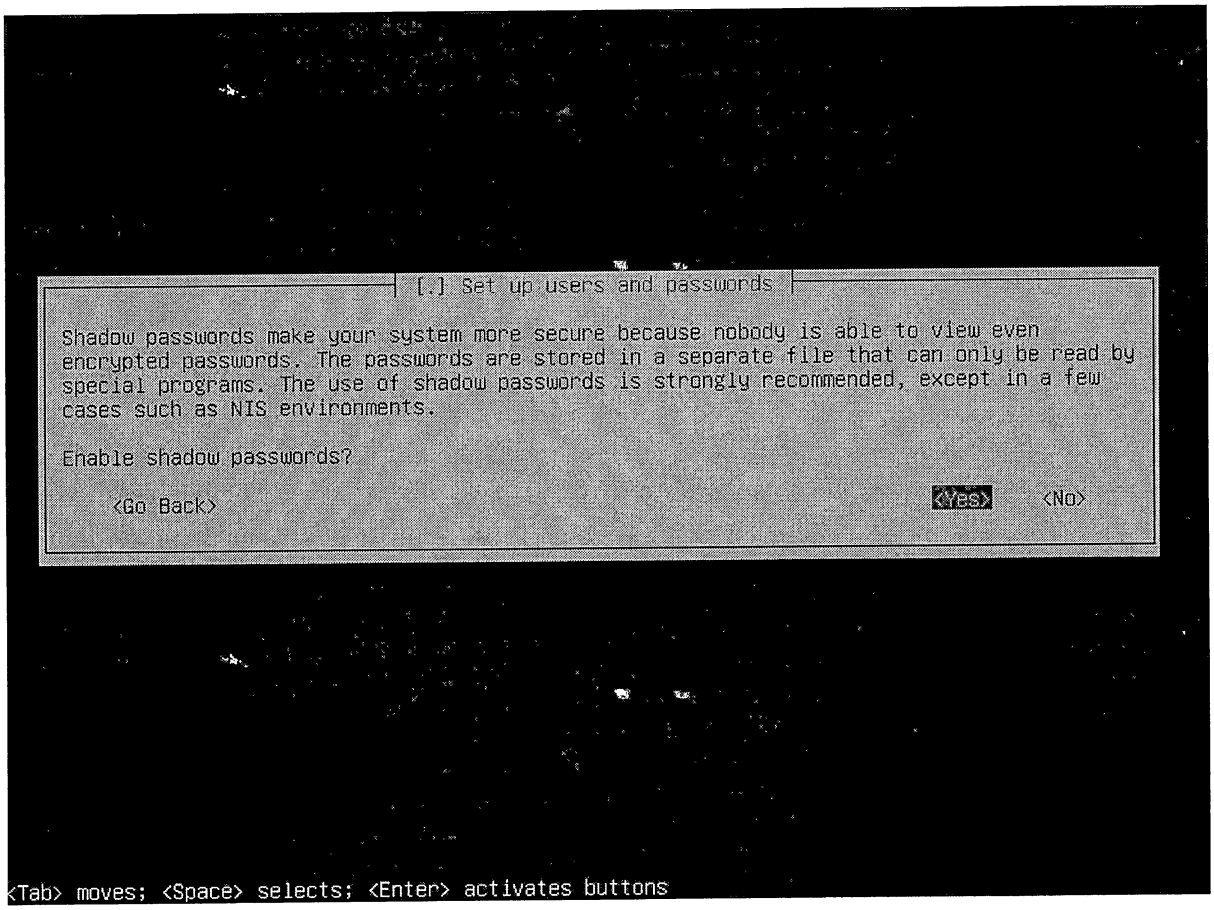
تنظیم کردن برایپسورد کاربر root مهمترین و اساسی ترین نیازمندی برای فراهم کردن امنیت یک سیستم است. در انتخاب پسورد root باید نهایت دقت را به کار بست و قوی ترین پسورد ممکن را انتخاب کرد. یک پسورد خوب:

- باید طول مناسب داشته باشد (حداقل ۱۵ کاراکتر)
- شامل ترکیبی از تمامی کاراکترهای ممکن مانند حروف کوچک و بزرگ و غیره باشد.
- پسورد نباید بر اساس اطلاعات شخصی مانند نام، نام پدر، نام همسر، شماره شناسنامه، شماره موبایل و غیره تعیین شود.
- برای تولید پسوردها مناسب می‌توان از ابزارهای خودکار مانند makepassd، pwgen وغیره استفاده کرد.

ردیف ۲-۷: فعال کردن Shadow password در حین نصب

با فعال کردن shadow password پسورد به صورت رمز شده و نمک زده شده (چند کاراکتر تصادفی به صورت خودکار اضافه می‌شود) در /etc/shadow/ ذخیره می‌شود و فقط کاربر root و گروه shadow حق دسترسی به این

فایل را دارند. هنگام نصب خودکار debian 7 از Sha512 استفاده می‌کند که دارای رمزگذاری محکم تری نسبت به md5 است. همان طور که در شکل مشاهده می‌کنید در انتهای نصب سیستم عامل shadow password را فعال کنید.



ردیف ۲-۸: نصب حداقل سرویس‌ها

هنگام نصب سیستم عامل باید سعی شود حداقل تعداد سرویس‌ها نصب شود. چرا که هر سرویس دارای آسیب پذیری‌هایی است که نصب آن‌ها می‌تواند امنیت سیستم را با خطر مواجه کند. سرویس‌هایی که باید در نصب آن‌ها حساسیت ویژه‌ای به خرج داد، سرویس‌های شبکه هستند. بعد از نصب سیستم عامل Debian، چنانچه سرویس اضافه‌ای نصب شده باشد، باید حذف شود. برای حذف/نصب سرویس‌های جدید شبکه می‌توان از super daemon مربوط به /etc/inetd.conf استفاده کرد. یا می‌توان سرویس جدید را در /etc/init.d/ اضافه کرده و symbolic linkهای آن‌ها را ایجاد کرد. همچنین باید دیمون‌های آسیب پذیری که به یک پورت خاص گوش می‌دهند، نیز غیر

فعال شوند. یک روش غیر فعال کردن دیمون‌ها استفاده از دستور update-rc.d است که به شکل زیر استفاده می‌شود:

Update-rc.d name stop XX 2

در این دستور name نام دیمون را مشخص می‌کند و XX زمان stop شدن سرویس را مشخص می‌کند. در نهایت برای پاک کردن سرویس می‌توان script مربوط به سرویس را در مسیر /etc/init.d/ را پاک کرد و سپس دستور زیر را وارد کرد:

Update-rc.d name remove

ردیف ۲-۹: نصب حداقل نرم‌افزارها

پس از نصب سیستم عامل باید حداقل تعداد نرم افزارهای مورد نیاز نصب شوند. نصب هر نرم‌افزار اضافه ممکن است امنیت سیستم را به مخاطره انداخته و مهاجم را در دسترسی به سیستم کمک کند. بنابراین باید سعی شود حداقل تعداد ممکن نرم افزارها نصب شود. نصب typical سیستم عامل debian سبب می‌شود تا تعداد زیادی نرم‌افزار به صورت پیش فرض نصب شود که بسیاری از آن‌ها مورد استفاده قرار نمی‌گیرد. بنابراین توصیه می‌شود که نصب debian به صورت سفارشی پیگیری شود. اگر نصب به صورت پیش فرض پیگیری می‌شود، توصیه می‌شود packageهای زیر حذف شوند:

- gdb
- gcc-3.3
- dpkg-dev
- libc6-dev
- cpp-3.3
- manages-dev
- flex
- g++
- linux-kernel-header
- bin86
- cpp
- gcc
- g++-3.3

- bison
- make
- libstdc++5-3.3-dev

و حذف زبان اسکریپت نویسی Perl در صورت امکان.

ردیف ۳-۱-۱: به‌روزرسانی وصله‌های امنیتی

برای به‌روزرسانی وصله‌ها دو راه وجود دارد: به صورت **online** که پس از نصب سرور باید سیستم را به اینترنت متصل کرد و به روز رسانی را انجام داد. برای به‌روزرسانی می‌توان خط زیر را به فایل source.list اضافه کرد:

deb http://security.debian.org/[CODENAME]/updates main contrib non-free

در دستور بالا به جای codename باید نام release مورد استفاده قرار گیرد (مانند squeeze). اکنون می‌توان از یکی از دستورات زیر برای به روز رسانی استفاده کرد:

aptitude update

aptitude upgrade

یا

Apt-get update

Apt-get upgrade

و به صورت **offline**: که باید آخرین وصله‌های امنیتی را از طریق یک سیستم دیگر گرفته و به صورت offline بر روی سرور نصب کرد. برای این کار می‌توانید یک Repository محلی ایجاد کنید. این روش برای به روز رسانی بسیار مناسب‌تر است.

ردیف ۳-۱-۲: به‌روزرسانی کتابخانه‌ها

هنگام به‌روزرسانی سرور ممکن است بعضی سرویس‌ها upgrade شوند و یا کتابخانه‌های جدیدی را جایگزین کتابخانه‌های آسیب پذیر خود کنند. برای اعمال این تغییرات جدید می‌بایست سرویس را restart کرد. چرا که در غیر این صورت ممکن است تغییرات جدید در سرویس اعمال نشود و سرویس همچنان دارای آسیب پذیری سابق

باشد. برای تشخیص اینکه چه سرویس‌هایی نیازمند restart شدن هستند، میتوان از ابزار checkrestart استفاده کرد و یا از دستور زیر استفاده کرد:

lsof | grep <the_upgraded_library> | uniq | sort -k

ردیف ۳-۱-۳: اضافه کردن وصله‌های هسته

سیستم عامل Debian برخی وصله‌ها را برای هسته لینوکس فراهم کرده است که امنیت آن را افزایش می‌دهد. لازم است در این گام این وصله‌ها را اضافه کنید که عبارتند از:

- Linux Intrusion detection که در بسته[۱۴] kernel-patch-2.4-lids وجود دارد. تمرکز این وصله روی لیست کنترل دسترسی است و قابلیت محافظت از فایل‌های مهم، دستگاه‌های I/O و پروسه‌ها را فراهم کرده است.
- Linux trustees که در بسته trustees فراهم شده است. این وصله سیستم مدیریت پیشرفته مجوزها را به هسته لینوکس اضافه می‌کند. به هر دایرکتوری یا فایل یک trustee پیوست می‌شود که قابل ارثبری توسط تمامی زیر دایرکتوری‌های آن است. به عبارت دیگر مجوز فایل‌های مختلف بدون در نظر گرفتن صاحب آن برای کاربران و گروه‌های مختلف کاربران در یک فایل پیکرردیف ی تعریف می‌شود.
- وصله exec-shield که در بسته kernel-patch-exec-shield فراهم است. این وصله در برابر برخی از سرریزهای بافر، سیستم را محافظت می‌کند.
- وصله Grsecurity در بسته kernel-patch-2.4-grsecurity و kernel-patch-grsecurity2 فراهم است که کنترل دسترسی اجباری را انجام می‌دهد و محافظت از سرریز بافر را از طریق ACL انجام می‌دهد.
- حمایت از IPSEC در هسته که در بسته linux-patch-openswan فراهم شده است. در صورت نیاز به استفاده از پروتکل IPSec در سیستم، لازم است این وصله نصب گردد. قابلیت‌های IPsec در هسته نسخه ۲,۵ اضافه شده و از نسخه ۲,۶ به بعد به صورت پیش فرض موجود است.
- وصله cryptoloop-source که از توابع kernel crypto API برای رمزنگاری سیستم فایل استفاده می‌کند.

ردیف ۳-۲-۱: امن‌سازی سرویس ssh

---

[14] Package

برای امن کردن ارتباط سرور SSH باید تغییرات مناسب را در فایل /etc/ssh/sshd_config اعمال کرد. مهمترین تغییراتی که می‌توان در این فایل اعمال کرد عبارتند از:

- **ListenAddress 192.168.0.1**: اگر چندین interface در سرور وجود داشته باشد و فقط بخواهیم که سرویس ssh به یک interface (192.168.0.1) گوش دهد. به عبارتی دیگر فقط کاربر بتواند به یک interface ارتباط ssh داشته باشد.
- **PermitRootLogin no**: کاربر نتواند به صورت مستقیم با استفاده از حساب root به سرور ssh بزند. با استفاده از این گزینه امکان حملات پسورد علیه کاربر root به صورت مستقیم وجود ندارد.
- **Port 666(or ListenAddress 192.168.0.1:666)**: تغییر پورت پیش فرض ssh. بدین ترتیب حمله‌گر از اجرای دیمون Sshd روی سیستم اطمینان ندارد.
- **AllowUsers alex ref me@somewhere**: فقط به کاربران خاصی اجازه ارتباط ssh داده می‌شود.
- **AllowGroups wheel admin**: فقط به گروه خاصی اجازه ارتباط ssh داده می‌شود.
- **PasswordAuthentication yes**: اگر این گزینه yes باشد کاربران می‌توانند پسورد خود را وارد کنند و احراز هویت شوند. اگر این گزینه no باشد، احراز هویت فقط با استفاده از کلید انجام می‌شود.
- می‌توان هر نوع خاصی از روش‌های احراز هویت را که لازم ندارید غیر فعال کنید. به عنوان مثال HostbasedAuthentication, RhostsRSAAuthentication, KerberosAuthentication را غیر فعال کرد.
- **Protocol 2**: غیر فعال کردن پروتکل نسخه ۱ به علت داشتن برخی نقص‌ها و امکان شکستن پسورد در آن.

ردیف ۳-۲-۲: امن کردن سرویس FTP

اگر حتما به سرویس Ftp نیاز دارید باید ریشه Ftp را با استفاده از chroot به دایرکتوری خانه کاربران ftp تغییر دهید تا کاربر نتواند جایی غیر از دایرکتوری خود را ببیند. می‌توانید در فایل proftpd.conf در قسمت عمومی خط زیر را اضافه کنید:

#DefaultRoot ~

در مرحله بعد سرویس proftpd را ریست کنید. Ftp اطلاعات لاگین را به صورت متن واضح میفرستد. برای امنیت بیشتر می‌توانید از Sftp استفاده کنید.

ردیف ۳-۲-۳: دسترسی امن به سیستم پنجره X

امروزه، ترمینال‌های X توسط بسیاری از سازمان‌ها برای استفاده از یک سرور در ایستگاه‌های کاری مختلف استفاده می‌شود. این مکانیزم به نوبه خود خطرناک است و اگر طبق اکثر مستندات عمل کنید با دستور xhost + می‌توانید از این مکانیزم استفاده کنید. که البته پیشنهاد نمی‌شود. در حالت بهتر می‌توانید از دستور xhost +hostname برای اتصال hostnameهای خاص به سرور استفاده کنید. راه‌حل بهینه برای این کار استفاده از Ssh جهت رمزنگاری کل جلسه است. برای این کار در سیستم کلاینت، در فایل /etc/ssh/ssh_config فیلد ForwardX11 را yes می‌کنیم. در سرور نیز فیلد X11Forwarding را yes می‌کنیم. اگر به دسترسی X از ماشین‌های دیگر نیاز ندارید با دستور زیر گوش کردن به پورت ۶۰۰۰ Tcp را غیرفعال کنید.

```
$startx -- -nolisten tcp
```

ردیف ۳-۲-۴: غیر فعال کردن NIS

برای حفظ امنیت پسوردهای سرور باید سرویس NIS غیر فعال شود. نحوه غیرفعال کردن در ردیف ۲-۸ توضیح داده شده است.

ردیف ۳-۲-۵: امن‌سازی سرویس RPC

سرویس‌های مبتنی بر RPC سوراخ امنیتی دارند و برخی از حملات DDOS از exploit های RPC برای وارد شدن به سیستم استفاده می‌کنند و به عنوان در دست گیرنده[۱۵] رفتار می‌کنند. اگر به RPC نیاز ندارید بهتر است با غیرفعال کردن سرویس portmap کاملا آن را غیرفعال کنید. وگرنه از راه‌های زیر دسترسی به آن را محدود کنید:

- بلوکه کردن دسترسی به پورت‌های استفاده شده توسط سرویس‌ها با استفاده از فایروال

---

[15] Handler

- بلوکه کردن دسترسی به این سرویس‌ها با استفاده از tcpwrapper
- می‌توانید بسته portmap را طوری پیکربندی کنید که تنها روی loopback interface گوش دهد. تا بتوانید سرویس‌های محلی RPC را استفاده کنید و درعین حال مانع از دسترسی سیستم‌ها از راه دور شوید.

ردیف ۳-۲-۶: تنظیمات مربوط به فایروال بر اساس نیازمندی‌ها

برای تنظیم قوانین فایروال می‌توانید از netfilter استفاده کنید. Netfilter چارچوبی برای دستکاری و حائل شدن بسته‌های شبکه است که به عنوان فایروال نیز می‌توان از آن استفاده کرد. UFW برای تنظیم و پیکربندی iptables در سیستم‌های Ubuntu استفاده می‌شود که معمولا به طور پیش فرض نصب است، اما در Debian بهتر است از shorewall استفاده کنید.

ردیف ۳-۲-۸: chroot کردن سرویس‌های تحت شبکه

برای اتوماتیک کردن روند chroot کردن می‌توان از ابزارهای موجود مانند makejail و compartment استفاده کرد.

ردیف ۳-۳-۱: تنظیم پسورد برای Grub

مهمترین وظیفه GRUB بارگذاری کردن هسته سیستم عامل است و اطلاعات مورد نیاز برای بارگذاری هسته را از مسیر /boot/grub/ می‌خواند. مهمترین اطلاعاتی که GRUB نیاز دارد، عبارتند از:

- Image مربوط به هسته: هسته به صورت یک image فشرده شده ذخیره می‌شود و GRUB باید آدرس این image را پیدا کند و آن را بارگذاری کند. ممکن است در یک سیستم چندین image وجود داشته باشد. که کاربر می‌تواند یکی از آن‌ها را انتخاب کند.
- Image مربوط به initrd یک سیستم فایل اولیه است که هنگام بارگذاری هسته، mount می‌شود. در واقع initrd شامل یک مجموعه کمینه از پوشه‌ها و فایل‌های اجرایی است که دسترسی به سیستم فایل اصلی و اجرای دستورات محدودی را برای کاربر فراهم می‌آورد. initrd قبل از mount شدن سیستم فایل اصلی بارگذاری می‌شود و در واقع پلی است بین بارگذاری هسته و mount شدن سیستم اصلی.

کاربر می‌تواند پس از بارگذاری شدن GRUB به صورت دلخواه یک هسته و initrd را بارگذاری کند. به عنوان مثال:

```
Grub> kernel  /bzimage-2.6.14.2
   [Linux-bzimage, setup=0x1400,  size=0x29672e]
Grub>initrd   /initrd-2.6.14.2.img
[linux-initrd @ 0x5f13000, 0xcc199 bytes]
Grub> boot
Uncompressing linux … ok, booting  the kernel.
```

همانطور که نشان داده شد کاربر می‌تواند با دسترسی به Grub، هسته مورد نظرش را mountکند. برای جلوگیری از این موضوع باید برای grub یک پسورد تنظیم کرد.

برای تنظیم پسورد برای Grub باید فایل /etc/grub.d/00_header را باز کرده خطوط زیر را اضافه کرد:

```
Cat<<EOF
set superuser=”test”
password_pbkdf2 test “رمز هش شده”
```

در خطوط بالا test نام کاربر است و برای تولید رمز هش شده از دستور زیر استفاده می‌شود:

```
grub-mkpasswd-pbkdf2
```

پس از وارد کردن دستور بالا از شما می‌خواهد یک پسورد را دو بار وارد کنید که با وارد کردن پسورد پس از چند دقیقه یک پسورد هش شده تولید می‌کند. حال باید این پسورد را به جای عبارت "رمز هش شده" در بالا وارد کرده و فایل را ذخیره نمود.

همچنین برای تنظیم پسورد برای منوهای GRUB باید خط زیر را

```
Printf “ menuentry ‘${title}’ $ {CLASS} { \n “ “ ${os}” “ ${version}”
```

در فایل /etc/10_linux به صورت زیر تغییر داد

```
Printf “ menuentry ‘${title}’ $ {CLASS}  --users test { \n “ “ ${os}” “ ${version}”
```

که test نام کاربر است.

همچنین برای حذف حالت recovery باید در فایل /etc/default/grub گزینه زیر را در حالت uncommented قرار داد:

```
GRUB_DISABLE_LINUX_RECOVERY=”true”
```

و بالاخره در فایل مقدار متغیر زیر را صفر قرار داد:

Set timeout=0

برای اعمال آخرین تغییرات کافی است دستور زیر را وارد کرد:

update-grub

ردیف ۳-۳-۲: محدود کردن ریبوت سیستم صرفا از طریق کنسول

هنگام خارج شدن از حساب کاربری یک کاربر ممکن است بدون لاگین کردن بتواند با استفاده از crtl+alt+del سیستم را ریبوت کند. برای جلوگیری از مشکل باید اطمینان حاصل شود که در فایل /etc/inittab فرمان shutdown با سوییچ a– استفاده شده است. مقدار ذخیره شده در این فایل باید به صورت زیر باشد:

ca: 12345: ctrlaltdel:/sbin/shutdown -t1 -a -r now

ردیف ۳-۳-۳: محدود کردن اجازه دسترسی به cron به کاربر root

دیمون cron برای زمان‌بندیِ پروسه‌ها استفاده می‌شود. دستور Crontab جهت ایجاد نمونه‌های crontab برای حساب root یا کاربران دیگر استفاده می‌شود. برای افزایش امنیت Cron بایستی فایل‌های cron.deny و cron.allow را جهت کنترل استفاده از Crontab پیکربندی کرد:

#cd /etc /

#/bin/rm -f cron.deny at.deny

#echo root >cron.allow

#echo root >at.allow

#/bin/chown root:root cron.allow at.allow

#/bin/chmod 400 cron.allow at.allow

ردیف ۳-۳-۴: استفاده از Tcpwrapper

استفاده از tcpwrapper به شرطی امکان‌پذیر است که سرویس از کتابخانه libwrap0 استفاده کند. برای مشاهده اینکه چه سرویس‌هایی از این کتابخانه استفاده می‌کنند می‌توان از دستور زیر استفاده کرد:

apt-cache rdepends libwrap0

- در فایل /etc/hosts.allow می‌توان مشخص کرد که چه کاربرانی به چه سرویس‌هایی دسترسی داشته باشند و در فایل /etc/hosts.deny می‌توان کاربرانی که حق استفاده از سرویس‌هایی را ندارند، بیان کرد. برای تنظیم کردن این مشخصات نیاز به توپولوژی شبکه و شناخت کاربران است.
- می توان هنگام trigger شدن یک سرویس توسط یک کاربر غیر مجاز یک Alert تولید کرده و در syslog ذخیره کرد. برای این منظور در فایل /etc/hosts.deny خطوط زیر را وارد می‌کنیم:

```
ALL: ALL: SPAWN\ )
echo -e "\n\
TCP Wrappers\: Connection refused\n\
By\: $(uname -n)\n\
Process\: %d (pid %p)\n\
User\: %u\n\
Host\: %c\n\
Date\: $(date)\n\
/ | "usr/bin/echo  "Connection to %d blocked" >>/var/log/syslog
```

ردیف ۳-۳-۵: اطمینان از عدم وجود دایرکتوری‌های null و یا مسیرهای نسبی در PATH مربوط به root

مسیر فعال در هر حساب کاربری، با لاگین به سیستم با همان حساب و اجرای دستور زیر انجام می‌شود:

```
#Echo $PATH
```

این دستور را برای حساب root چک کنید. برای هر دایرکتوری خروجی، مطمئن شوید که شامل کاراکتر نقطه به تنهایی، و یا نمونه‌هایی از مسیرهای نسبی مانند .. نباشد و تمامی مسیرها با / شروع شود. در عین حال مطمئن شوید که عنصر خالی در مسیرها وجود نداشته باشد که به منزله همان نقطه هستند. مثل گزینه زیر:

```
PATH=:/bin
PATH=/bin:
PATH=/bin::/sbin
```

ردیف ۳-۳-۶: اطمینان از عدم وجود مجوز world-writable یا group-writable در مدخل‌های PATH مربوط به root

به ازای هر یک از عناصر درون PATH دستور زیر را اجرا کنید:

```
# ls -ld DIR
```

و مطمئن شوید که مجوز نوشتن برای گروه و دیگران غیر فعال است.

ردیف ۳-۳-۷: اطمینان از عدم قابلیت نوشتن توسط گروه و دیگران برای دایرکتوری home کاربران

برای هر کاربر سیستم، مجوزهای دایرکتوری home کاربر را مشاهده کنید:

```
# ls -ld /home/USER
```

مطمئن شوید که همه دایرکتوری‌ها قابلیت نوشتن توسط گروه و خواندن توسط دیگران را ندارند:

```
# chmod g-w /home/USER
# chmod o-rwx /home/USER
```

دایرکتوری home کاربران شامل تعداد زیادی فایل پیکربندی هستند که رفتار حساب کاربری را تحت تاثیر قرار می‌دهند. هیچ کاربری حق نوشتن در دایرکتوری کاربر دیگر را ندارد. اگر نیاز به دایرکتوری به اشتراک گذاشته شده در گروه حس می‌شود، می‌تواند در قسمتی دیگر از سیستم فایل پیکربندی شود.

ردیف ۳-۳-۸: اطمینان از عدم وجود مجوز world-writable در فایل‌های دات[16] (پنهان) کاربر

برای هر کاربر سیستم، مجوزهای فایل‌های نقطه‌دار را در دایرکتوری home آن‌ها مشاهده کنید.

```
# ls -ld /home/USER /.[A-Za-z0-9]*
```

و مطمئن شوید که هیچ یک قابلیت نوشتن توسط گروه و دیگران را ندارند. با دستور زیر هر گونه مجوز اشتباه را اصلاح کنید:

```
# chmod go-w /home/USER /FILE.
```

---

[16] Dot-files

ردیف ۳-۳-۹: تنظیم پارامترهای انقضای پسورد

باید فایل /etc/login.defs را جهت تنظیمات انقضا برای کاربران جدید ویرایش کرد. خطوط زیر را اضافه کرده یا اصلاح کنید:

PASS_MAX_DAYS 60
PASS_MIN_DAYS 7
PASS_MIN_LEN 14
PASS_WARN_AGE 7

برای USER هایی که قبلا ایجاد شده‌اند دستور زیر را اجرا کنید:

chage -M 60 -m 7 -W 7 USER

پارامتر PASS MAX DAYS(-M) ماکزیمم زمانی را تنظیم می‌کند که کاربر می‌تواند از یک پسورد استفاده کند و پس از آن میبایست آن را تغییر دهد. این امر جهت کاهش بهره‌برداری از پسوردهای مورد حمله واقع شده است. پارامتر PASS MIN DAYS (-m) مانع از تغییر پسورد به مدت ۷ روز پس از اولین تغییر می‌شود. پارامتر The PASS WARN AGE (-W) تعداد روزهای اخطار به کاربر در زمان لاگین را مبنی بر انقضای پسورد، مشخص می‌کند.

ردیف ۳-۳-۹: تنظیم پارامترهای طول و پیچیدگی پسورد

با فعال کردن ماژول pam_cracklib می‌توان کمترین طول پسورد و به طور ضمنی پیچیدگی آن را برای کاربرانی که از این به بعد تعریف می‌شوند تنظیم کرد. این ماژول با نصب کتابخانه libpam_cracklib به سیستم اضافه می‌شود و پیکربندی زیر را به فایل /etc/pam.d/common-password اضافه می‌کند:

Password requisite pam_cracklib.so retry=3 minlength=8 difok=3

اگر مایل به تغییر مقادیر پیش فرض آن هستید می‌توانید آن‌ها را تغییر دهید. این ماژول طول کمینه و استحکام پسورد را به طور ترکیبی دیده است. یعنی پسورد باید طول حداقلی ۸ کاراکتر داشته باشد و قوی باشد. فیلد difok نیز نشان دهنده تعداد کمینه کاراکترهای متفاوت در پسورد جدید نسبت به پسورد قبلی است.

ردیف ۳-۴-۱: محدود کردن مجوز پارتیشن‌های مختلف

پس از پارتیشن‌بندی، باید مجوزهای لازم را برای هر پارتیشن تنظیم کرد. به عنوان مثال برای پارتیشن tmp/ باید مجوز nosuid و noexec را تنظیم کرد تا به کاربر اجازه اجرای برنامه در این پارتیشن را ندهد و فقط کاربر root حق دسترسی write را داشته باشد. ذکر این نکته بسیار مهم است که ابتدا باید برنامه را نصب کرد و تنظیمات لازم را انجام داد سپس مجوز پارتیشن‌های مختلف را تعیین کرد. به عنوان مثال اگر مجوزهایی که برای tmp/ عنوان شد قبل از نصب نرم افزارها انجام شود ممکن است سبب اخلال در نصب نرم افزارهای جدید شود. چرا که برنامه‌هایی نظیر apt از این مسیر به عنوان مسیر موقت برای نصب برخی نرم افزارها استفاده می‌کنند. بنابراین یا باید پس از نصب فایل‌ها این مجوزها را تعیین کرد و یا مسیر مورد استفاده apt را در فایل /etc/apt/apt.conf تغییر داد. در ادامه چند نمونه از مجوزهای مورد نیاز برای هر پارتیشن ارائه شده است (این نمونه‌ها عینا در فایل /etc/fstab برای mount شدن پارتیشن‌ها می‌آیند.):

/dev/sda6 /usr ext3 defaults,ro,nodev 0 2

/dev/sda12 /usr/share ext3 defaults,ro,nodev,nosuid 0 2

/dev/sda7 /var ext3 defaults,nodev,usrquota,grpquota 0 2

/dev/sda8 /tmp ext3 defaults,nodev,nosuid,noexec,usrquota,grpqu

/dev/sda9 /var/tmp ext3 defaults,nodev,nosuid,noexec,usrquota,grpqu

/dev/sda10 /var/log ext3 defaults,nodev,nosuid,noexec 0 2

/dev/sda13 /home ext3 rw,nosuid,nodev,exec,auto,nouser,async,usrq

/dev/fd0 /mnt/fd0 ext3 defaults,users,nodev,nosuid,noexec 0

/dev/fd0 /mnt/floppy vfat defaults,users,nodev,nosuid,noexec 0

/dev/hda /mnt/cdrom iso9660 ro,users,nodev,nosuid,noexec 0

البته apt دارای یک ویژگی جالب است که می‌تواند قبل از نصب، پارتیشن را remount کرده و مجوزهای لازم برای نصب نرم افزار را صادر کند و پس از نصب نرم افزار دوباره مجوزها را به حالت قبل برگرداند. برای این منظور باید تنظیمات لازم را در فایل /etc/apt/apt.conf انجام داد. مثلاً برای نصب نرم افزار نیاز به مجوز write است اگر پارتیشن usr/ دارای مجوز read باشد امکان نصب وجود ندارد. بنابراین نیاز به تغییرات زیر است:

```
DPkg
{
Pre-Invoke { "mount /usr -o remount,rw”};
Post-Invoke { "mount /usr -o remount,ro”};
}
```

ردیف ۳-۴-۲: بررسی و تایید مجوز فایل‌های shadow، Group، gshadow و passwd:

```
# cd /etc
# chown root:root passwd shadow group gshadow
# chmod 644 passwd group
# chmod 400 shadow gshadow
```

بسیاری از برنامه‌ها برای کارکرد صحیح نیاز به دسترسی خواندن فایل passwd دارند، اما دسترسی خواندن فایل Shadow باعث حملات مخرب به پسوردهای سیستم می‌شود و هرگز نباید اجازه داده شود.

ردیف ۳-۴-۳: بررسی تمامی دایرکتوری‌های قابل world-writable برای داشتن بیت‌های Sticky

تمامی دایرکتوری‌های پارتیشن‌های مختلف را جستجو کنید و چک کنید که اگر قابل نوشتن برای همه هستند حتما بیت sticky آن‌ها تنظیم شده باشد:

دستور زیر را برای همه پارتیشن‌های PART اجرا کنید:

```
# find PART -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
```

اگر دستور قبلی خروجی داشت، به ازای هر dir خروجی دستور بعدی را اجرا کنید:

```
# chmod +t /dir
```

راه‌حل بهتر به جای تنظیم بیت sticky حذف دسترسی نوشتن توسط همه افراد است.

ردیف ۳-۴-۴: یافتن فایل‌های world-writable غیر مجاز

با دستور زیر تمامی فایل‌های قابل نوشتن توسط همه را در پارتیشن‌ها پیدا کنید:

```
# find PART -xdev -type f -perm -0002 -print
```

و به ازای همه آن‌ها مجوز را تغییر دهید، به طوری که تنها مالک آن‌ها حق نوشتن داشته باشد:

```
# chmod o-w file
```

ردیف ۳-۴-۵: یافتن فایل‌های بدون مالک و اصلاح آن‌ها

دستور زیر تمامی فایل‌های بدون مالک را پیدا می‌کند. لازم است هر یک از خروجی‌های این دستور بررسی شده و به کاربر و گروه معتبری نسبت داده شود و یا کلا حذف شود.

```
# find PART -xdev \( -nouser -o -nogroup \) -print
```

فایل‌های بدون مالک به خودی خود قابل بهره‌برداری نیستند، اما نشانه‌ای از مشکل در پروسه‌های سیستم است. این امر ممکن است توسط یک نفوذی انجام شده باشد و یا به علت نصب یا حذف نادرست و یا ناکامل نرم‌افزار اتفاق افتاده باشد و یا به علت حذف شکست خورده فایل‌های مربوط به یک حساب کاربری ایجاد شده باشند.

ردیف ۳-۴-۶: بررسی تمامی دایرکتوری‌های world-writable جهت صحیح بودن مالکیت آن‌ها

دستور زیر را برای پارتیشن‌های PART اجرا کنید و به ازای تمامی خروجی‌ها چک کنید که مالک آن‌ها root یا حساب‌های کاربری سیستمی باشد.

```
# find PART -xdev -type d -perm -0002 -uid +500 –print
```

ردیف ۳-۴-۷: کمینه کردن برنامه‌های SetUID/SetGID

برنامه‌هایی که SetUID یا SetGID هستند کاندید خوبی برای حذف از سیستم هستند، چرا که هر باگی در این برنامه‌ها تاثیر امنیتی دارد و به حمله‌گری که خود قبلا به سیستم دسترسی داشته است اجازه می‌دهد امتیازش را افزایش دهد و کنترل خود را روی سیستم بالا ببرد.

- تمامی برنامه‌های SetUID/SetGID را روی سیستم با دستور find / -perm +6000 –ls پیدا کنید.
- ترجیحا اگر آن‌ها را نیاز ندارید حذف کنید.
- در غیر این صورت بیت SetUID یا SetGID را غیرفعال کنید تا برنامه تنها امتیاز کاربری که آن را اجرا می‌کند داشته باشد.

اگر واقعا نیاز است که این برنامه‌ها توسط کاربران دیگر اجرا شوند، آن‌ها را با عضویت در گروه اجرا کنید:

- یک گروه جدید برای این برنامه بسازید.

#addgroup <group-name>

- گروه مالک برنامه را به گروه جدید ساخته شده تغییر دهید.

#chgrp <group-name> <program>

- مجوز برنامه را جهت رد مجوز اجرایی برای دیگران، تغییر دهید.

#chmod o-x <program>

- کاربرانی که لازم است این برنامه را اجرا کنند، به گروه جدید اضافه کنید.

#useradd –G <groupname> <username>

ردیف ۳-۵-۱: داشتن فرم کاغذی جهت ثبت نام کاربران برای حساب کاربری

هر سازمان بایستی فرم کاغذی جهت ثبت نام کاربران برای حساب کاربری توزیع کند که شامل امضای کاربر جهت مطالعه سیاست امنیتی سازمان و تعهد رعایت آن از طرف کاربر و مشمول عواقب تجاوز از سیاست‌ها می‌شود.

ردیف ۳-۵-۴: غیر فعال کردن هر گونه حساب بدون پسورد

دستور زیر وضعیت حساب کاربری را نشان می‌دهد:

#passwd –S <username>

اگر فیلد NP پس از نام کاربری نشان داده شود به معنی عدم داشتن پسورد است. و لازم است در صورت عدم نیاز به آن‌ها، حساب کاربریشان حذف شود و یا برای آن‌ها پسورد تنظیم شود.

ردیف ۳-۵-۷: از بین بردن پروسه‌های در حال اجرای کاربر حذف شده با شناسه UID

از دستور ps جهت چک کردن پروسه‌های در حال اجرا با UID کاربر مورد نظر استفاده کنید و آن‌ها را kill کنید.

دستور زیر را اجرا کنید:

awk -F: '($2 == "") {print}' /etc/shadow

اگر دستور بالا خروجی داشت، به ازای هر خروجی حساب کاربری را غیر فعال کنید.

ردیف ۳-۶-۱: پیکربندی جهت ثبت و جمع‌آوری لاگ فایل‌ها

فایل پیکربندی syslog را واقع در مسیر /etc/syslog.conf که به طور پیش‌فرض برخی از تنظیمات آن کامنت شده باز کرده و خطوط زیر را از حالت کامنت خارج کنید.

```
daemon,mail.*;\
        news.=crit;news.=err;news.=notice;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       /dev/tty8
```

و سپس سرویس Syslog را ریست کنید. Debian برخی ابزار تحلیل لاگ مانند Swatch, logchecker و یا log-analysis را فراهم کرده است که با پیکربندی صحیح می‌توانید از آن‌ها استفاده کنید. در عین حال لازم است محل ذخیره پیام‌های ارسالی توسط Syslog را مشخص کنید که معمولا یک سیستم جدا به نام loghost برای این کار در نظر گرفته می‌شود تا پیام‌ها را از راه دور تحت شبکه جمع‌آوری کند. در صورت حمله به سیستم مورد نظر، حمله‌گر نمی‌تواند ردپای خود را پاک کند (مگر اینکه به سیستم loghost نیز نفوذ کند.)

جهت پیکربندی سیستم به عنوان loghost باید فایل /etc/rsyslog.conf را باز کرده و خطوط

```
$ModLoad imudp
$UDPServerRun 514
```

یا

```
$ModLoad imTcp
$InputTCPServerRun 514
```

از حالت کامنت خارج کنید و سرویس Syslog را ریست کنید. برای پیکربندی ماشین‌های دیگر جهت فرستادن پیام‌ها به loghost باید در فایل /etc/rsyslog.conf خط زیر را اضافه کنید:

```
facility.level          @your_loghost
```

نهایتا مجوز دسترسی به فایل لاگ‌ها نیز پس از نصب سیستم‌عامل باید مورد بازبینی قرار گیرد. به طور مثال فایل /var/log/lastlog و /var/log/faillog به ترتیب آخرین لاگین به سیستم و خلاصه‌ای از لاگین‌های شکست خورده را گزارش می‌دهند که لزومی ندارد برای هر کاربر غیر root قابل خواندن باشد و می‌توان به آن‌ها Chmod 660 نسبت داد. نمونه‌ای از دستورات جهت چک کردن فایل‌های لاگ آمده است:

```
#  find /var/log -type f -exec ls -l {} \; | cut -c 17-35 |sort –u
```

(see to what users do files in /var/log belong)

find /var/log -type f -exec ls -l {} \; | cut -c 26-34 |sort -u

(see to what groups do files in /var/log belong)

find /var/log -perm +004

(files which are readable by any user)

find /var/log \! -group root \! -group adm -exec ls -ld {} \;

(files which belong to groups not root or adm)

ردیف ۳-۶-۲: انتقال داده تحت شبکه به صورت امن

برای انتقال فایل بین سیستم نصب شده و دیگر سیستم‌ها لازم است از روشی امن مانند بسته Ssh استفاده کنید. راه دیگر استفاده از ftpd-ssl است. هر یک از این روش‌ها کلاینت خاص خود را نیز لازم دارند. به طور مثال Scp از بسته Ssh و یا putty و winscp برای انتقال امن از سیستم‌های ویندوزی مناسب هستند. دقت داشته باشید که Scp دسترسی به تمام سیستم فایل را برای کاربران فراهم می‌کند مگر اینکه تنظیمات chroot را انجام دهید.

ردیف ۳-۶-۳: اعمال سیاست سهمیه‌بندی فضای دیسک

سیستم سهمیه‌بندی در لینوکس شامل دو نوع سهمیه کاربر و گروه است که به ترتیب مقدار فضای استفاده شده توسط کاربر و گروه را محدود به مقداری از پیش تعیین شده می‌کند. و سهمیه‌ها را در تمامی فضاهای قابل نوشتن کاربر مانند tmp/ و home/ اعمال کنید. جهت انجام این کار ابتدا باید اطمینان حاصل کنید که سهمیه‌بندی در هسته شما حمایت شود. سپس چک کنید که بسته quota نصب شده باشد. برای فعال‌سازی سهمیه‌بندی کاربر یا گروه کافیست به فایل etc/fstab/ رجوع کرده و به جای Defaults، به ترتیب defaults, usrquota و defaults, grpquota را جایگزین کنید. البته از هر دوی آن‌ها نیز می‌توانید استفاده کنید. سپس فایل‌های خالی quota.user و quota.group را در ریشه سیستم فایلی که می‌خواهید سهمیه‌بندی کنید ایجاد کنید. (به طور مثال، touch /home/quota.user /home/quota.group برای سیستم فایل home/). سپس سرویس quota را ریست کنید. اکنون می‌توانید با دستور edquota –u <user> و edquota –g <group> مقدار سهم‌ها را مشخص کنید.

ردیف ۳-۶-۴: چک کردن صحت فایل‌های سیستم:

برای اطمینان حاصل کردن از هرگونه تغییر فایل‌های سیستم لازم است به طور متناوب (روزانه) صحت آن‌ها چک شود. این کار با مقایسه md5sum قدیمی فایل‌ها و مقدار کنونی انجام می‌شود. ابزارهای معمول برای این کار،Aide، Tripwire، integrit و sxid است. نصب Debsums نیز با مقایسه md5sum فایل و نسخه مورد استفاده در debian package archive می‌تواند در تعیین صحت به شما کمک کند.

ردیف ۳-۶-۵: امن‌سازی دسترسی تحت شبکه:

برای مشاهده کل پارامترهای مربوط به هسته می‌توان از دستور زیر استفاده کرد.

Sysctl -A

این دستور تمامی متغیرهایی هسته که توسط کاربر تنظیم می‌شوند را نمایش می‌دهد. برای تنظیم کردن هر متغیر می‌توان از دستور زیر استفاده کرد:

Sysctl -w <Variable_name=value>

البته به ندرت از این متغیرها استفاده می‌شود ولی برخی مواقع می‌توان برای امن سازی سرویس از این پارامترها استفاده کرد.

- برای غیرفعال کردن ping به صورت broadcast باید به صورت زیر عمل کرد:

net/ipv4/icmp_echo_ignore_broadcasts = 1

- برای جلوگیری از پاسخ به درخواست‌های ping از دستور زیر استفاده می‌شود:

Sysctl –w net/ipv4/icmp_echo_ignore_all = 1

- همچنین برای ثبت log درخواست‌هایی که به دلیل عدم مسیریابی مناسب به مقصد نمی رسند، باید پارامتر زیر را تنظیم کرد:

/proc/sys/net/ipv4/conf/all/log_martians = 1

- برای جلوگیری از حملات packet flooding از گزینه زیر استفاده می‌شود که در هنگام افزایش لود بسته‌های syn برای صف یک طول معین تعریف می‌شود:

net/ipv4/tcp_syncookies = 1

- به طوری کلی خطوط زیر یک نمونه از تنظیمات امن پارامترهای هسته را نشان می‌دهد:

Be warned that /etc/init.d/procps is executed to set the following
#variables. However, after that, /etc/init.d/networking sets some

```
#network options with builtin values. These values may be overridden
#using /etc/network/options.
#kernel.domainname = example.com
#Additional settings - adapted from the script contributed
#by Dariusz Puchala (see below(
#Ignore ICMP broadcasts
net/ipv4/icmp_echo_ignore_broadcasts = 1
#Ignore bogus ICMP errors
net/ipv4/icmp_ignore_bogus_error_responses = 1
# Do not accept ICMP redirects (prevent MITM attacks(
net/ipv4/conf/all/accept_redirects = 0
#Accept ICMP redirects only for gateways listed in our default
#gateway list (enabled by default(
#net/ipv4/conf/all/secure_redirects = 1
#Do not send ICMP redirects (we are not a router(
net/ipv4/conf/all/send_redirects = 0
#Do not forward IP packets (we are not a router(
#Note: Make sure that /etc/network/options has 'ip_forward=no'
net/ipv4/conf/all/forwarding = 0
#Enable TCP Syn Cookies
#Note: Make sure that /etc/network/options has 'syncookies=yes'
net/ipv4/tcp_syncookies = 1
#Log Martian Packets
net/ipv4/conf/all/log_martians = 1
#Turn on Source Address Verification in all interfaces to
#prevent some spoofing attacks
#Note: Make sure that /etc/network/options has 'spoofprotect=yes'
net/ipv4/conf/all/rp_filter = 1
```

#Do not accept IP source route packets (we are not a router(

net/ipv4/conf/all/accept_source_route = 0

برای اعمال تغییرات فوق در هر مرحله از بوت شدن سیستم باید این خطوط در فایل /etc/sysctl.conf قرار داد.

پس از انجام این تغییرات در هر مرحله بوت شدن سیستم این تنظیمات به صورت خودکار اعمال می‌شوند.

همچنین می‌توان یک اسکریپت تهیه کرده برای هر interface این تنظیمات را به صورت جدا انجام داد. برای این منظور باید ابتدا در فایل /etc/network/interfaces به ازای هر interface فعال خط زیر را وارد کرد.

pre-up /etc/network/interface-secure

به عنوان مثال تنظیمات interface 0 به صورت زیر است:

auto eth0
iface eth0 inet static
address xxx.xxx.xxx.xxx
netmask 255.255.255.xxx
broadcast xxx.xxx.xxx.xxx
gateway xxx.xxx.xxx.xxx
pre-up /etc/network/interface-secure

حال باید اسکریپت مناسب برای ست کردن تنظیمات پارامترهای هسته نوشته و در مسیر /etc/network قرار داد.

به عنوان مثال اگر نام فایل secure-interface باشد باید این فایل را در مسیر /etc/network/secure-interface قرار داد. اسکریپت نوشته به صورت زیر است:

/!#bin/sh -e

#Script-name: /etc/network/interface-secure

#Modifies some default behavior in order to secure agains

#some TCP/IP spoofing & attacks for all interfaces.

#Contributed by Dariusz Puchalak.

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

#Broadcast ech

echo 0 > /proc/sys/net/ipv4/conf/all/forwarding

#IP forwarding

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# TCP syn cooki
echo 1 >/proc/sys/net/ipv4/conf/all/log_martians
# Log str ) #this includes spoofed packets, source routed packets, r
#but be careful with this on heavy loaded web servers.
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_respon
#Bad error mes
#IP spoofing protection.
echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
#Disable ICMP redirect acceptance.
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects
#Disable source routed packets.
echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
exit 0
```

ردیف ۳-۶-۶: گرفتن Snapshot از سیستم و پشتیبان‌گیری دوره‌ای از داده‌ها و سیستم فایل

پس از نصب موفقیت آمیز سیستم و اعمال تنظیمات مناسب اکنون باید یک snapshot از سیستم تهیه شود. چرا که در مواقعی که به خروجی سیستم مشکوک هستیم و یا می‌خواهیم از صحت عدم تغییر فایل‌های نصب شده اطمینان پیدا کنیم، میتوان md5 یا sha1 را مقادیر قبلی آنها را مقایسه کرد. برای تهیه snapshot از اسکریپت زیر استفاده می‌شود:

```
/!#bin/bash
/bin/mount /dev/fd0 /mnt/floppy
trap "/bin/umount /dev/fd0" 0 1 2 3 9 13 15
if [ ! -f /usr/bin/md5sum ] ; then
echo "Cannot find md5sum. Aborting".
exit 1
```

```
fi
/bin/cp /usr/bin/md5sum /mnt/floppy
echo "Calculating md5 database"
/<mnt/floppy/md5checksums.txt
for dir in /bin/ /sbin/ /usr/bin/ /usr/sbin/ /lib/ /usr/lib/
do
find $dir -type f | xargs /usr/bin/md5sum >>/mnt/floppy/md5checksums-lib.t
done
echo "post installation md5 database calculated"
if [ ! -f /usr/bin/sha1sum ] ; then
echo "Cannot find sha1sum "
echo "WARNING: Only md5 database will be stored"
else
/bin/cp /usr/bin/sha1sum /mnt/floppy
echo "Calculating SHA-1 database"
>/mnt/floppy/sha1checksums.txt
for dir in /bin/ /sbin/ /usr/bin/ /usr/sbin/ /lib/ /usr/lib/
do
find $dir -type f | xargs /usr/bin/sha1sum >>/mnt/floppy/sha1checksums-lib
done
echo "post installation sha1 database calculated"
fi
exit 0
```

این اسکریپت با فرض ذخیره کردن md5 در فلش یا دیسک نرم تهیه شده است. در عین حال لازم است به صورت دوره‌ای با ابزارهای پشتیبان‌گیری از اطلاعات خود پشتیبان تهیه کنید.

ردیف ۳-۶-۷: محافظت در برابر حملات ARP

جهت محافظت در برابر حملات ARP راه‌حل‌های زیر پیشنهاد می‌شود:

۱. از کش ایستای ARP برای هر سیستم مهم در شبکه خود استفاده کنید: Arp –s host_name hdwr_addr. با این کار میزبان‌های شبکه داخلی شما به طور دستی تنظیم می‌شوند. و پاسخ spoof ARP شده نیز نادیده گرفته می‌شود.

۲. ترافیک مشکوک ARP را توسط ابزارهای arpwatch یا IDSهای عمومی تشخیص دهید.

ردیف ۳-۶-۸: بنر هشداردهنده

اگر سیاست سازمان شما نیاز به بنر هشداردهنده دارد می‌توانید آن را در فایل‌های زیر کپی کنید:

/etc/motd

/etc/issue

/etc/issue.net

add 'GreetString=”Authorized Use Only”" to /etc/X11/xdm/kdmrc and

make a similar change to gdm.conf

به طور مثال این یک پیغام بنر است: "به طور مجاز از سیستم استفاده کنید. تراکنش‌ها پایش می‌شوند."

ردیف ۳-۶-۹: محافظت با آنتی‌ویروس

گزینه‌های آنتی‌ویروس قابل دسترسی متعددی برای کاربران لینوکس وجود دارد که تعداد آن‌ها نیز رو به افزایش است. از آن جمله می‌توان به ClamAV، f-prot و Vexira اشاره کرد.

ردیف ۳-۶-۱۰: غیر فعال کردن ipv6 در صورت عدم استفاده

از آن جایی که ipv6 مستعد حمله است اگر از آن استفاده نمی‌کنید لازم است غیر فعال کنید. فایل /etc/modprobe.d/aliases را باز کرده و خط زیر را کامنت کنید:

alias netpf10 off

و در فایل /etc/modprobe.d/blacklist خط زیر را اضافه کنید:

blacklist ipv6:

و در آخر چک کنید:

lsmod | grep ipv6

ردیف ۳-۶-۱۱: غیر فعال کردن Core dump

جهت غیر فعال کردن Core dump در فایل /etc/sysctl.conf خط زیر را اضافه یا ویرایش کنید:

fs.suid_dumpable = 0

فایل core dump یک image از حافظه برنامه قابل اجرا است که به علت رفتار انحرافی، سیستم عامل آن را به اتمام رسانده است. در اکثر مواقع تنها توسعه‌دهندگان نرم‌افزارها نیاز به دسترسی به این فایل‌ها دارند. در عین حال این فایل‌ها ممکن است حاوی اطلاعات حساس باشد و یا از نظر حجمی، مقدار زیادی از دیسک را اشغال کند.

ردیف ۳-۶-۱۲: بررسی صحت وصله‌ها و به‌روزرسانی‌ها قبل از نصب آن‌ها

قبل از نصب به روز رسانی‌ها و وصله‌ها، لازم است چک کنید که تغییری در آن‌ها اعمال نشده باشد.

- در برخی سیستم‌ها، امضای دیجیتال روی وصله‌ها وجود دارد که ممکن است به طور اتوماتیک توسط ابزار بسته تایید شود.
- برخی وصله‌ها و به‌روزرسانی‌ها امضای PGP دارند. این امضاها توسط GnuPG تایید می‌شوند.
- اگر امضای دیجیتال در دسترس نیست اما هش MD5 یا SHA آن موجود است، می‌توانید برای تایید صحت از آن استفاده کنید.