بیست نکته در امنیت

LINUX

شبکه گستر
امنیت شما | وظیفه ما

عنوان سند: بیست نکته در امنیت Linux
شناسه سند: SPT-A-0144-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ ویرایش: ۱۷ دی ۱۳۹۶

۱- حفاظت فیزیکی سیستم

علاوه بر تأمین حفاظت فیزیکی سرورهای تحت سیستم عامل Linux، غیرفعال کردن امکان بالا آمدن سیستم[۱] از روی CD/DVD، USB Flash و Floppy Disk در تنظیمات BIOS این دستگاه‌ها نیز توصیه می‌شود. اختصاص گذرواژه[۲] BIOS و قرار دادن گذرواژه بر روی راه‌انداز GRUB برای جلوگیری از دسترسی فیزیکی به اطلاعات سیستم نیز از دیگر نکاتی است که می‌بایست مدنظر قرار داده شود.

۲- نصب حداقل بسته‌ها

توصیه می‌شود بسته‌های نرم‌افزاری غیرضروری از روی سرور حذف شوند. وجود آسیب‌پذیری در هر یک از این بسته‌ها، امنیت کل سرور را به خطر می‌اندازد.

با استفاده از فرامین زیر می‌توان فهرست بسته‌های نرم‌افزاری نصب شده را مشاهده کرد:

در توزیع‌های Redhat	`sudo yum list installed`
در توزیع‌های Debian	`sudo dpkg --list`

برای حذف بسته‌های نصب شده نیز می‌توان از دستورات زیر استفاده کرد:

در توزیع‌های Redhat	`sudo yum remove <packageName>`
در توزیع‌های Debian	`sudo apt-get remove <packageName>`

۳- رمزنگاری ارتباطات شبکه

استفاده از پودمان SSL برای رمزگذاری ارتباطات سرویس‌های داخل شبکه و دسترسی‌های از راه دور سرویس‌ها و پودمان‌هایی همچون Apache یا OpenVPN توصیه می‌شود.

٤- عدم استفاده از پودمان‌های FTP، Telnet و Rlogin

پودمان‌های FTP، Telnet و Rlogin اطلاعات را به صورت متن ساده[۳] ارسال و دریافت می‌کنند؛ به همین دلیل دستورات و فایل‌ها می‌توانند توسط افراد غیرمجاز شنود و دریافت شوند. از SFTP و OpenSSH می‌توان به عنوان جایگزینی برای سرویس‌های مذکور استفاده کرد.

۵- استفاده از SSH

یکی از ساده‌ترین روش‌های دسترسی از راه دور به سیستم عامل Linux پودمان شبکه‌ای SSH است. در این پودمان، ارتباط میان ایستگاه کاری و سرور به صورت رمزنگاری و امن شده برقرار می‌شود. برای جلوگیری از ایجاد دسترسی افراد غیرمجاز به سرور از طریق پودمان SSH انجام مراحل زیر توصیه می‌شود.

الف) با اجرای فرمان زیر تنظیمات پودمان SSH از طریق فرمان زیر باز شود:

```
sudo nano /etc/ssh/sshd_config
```

ب) سپس با درج عبارت زیر ورود کاربر Root غیرفعال شود:

```
PermitRootLogin no
```

---

۱ Boot
۲ Password
۳ Clear Text

ج) کاربرانی را که از طریق SSH می‌توانند به سیستم وارد شوند تعیین شوند (کاربرانی که در فایل /etc/sudoers تعریف شده‌اند):

```
AllowUsers <username>
```

د) استفاده از نسخه ۲ پودمان SSH مشخص شود:

```
Protocol 2
```

هـ) درگاه پیش‌فرض این پودمان از ۲۲ به شماره‌ای دیگر و غیرقابل حدس زدن تغییر داده شود.

```
Port 5724
```

همچنین استفاده از کلید عمومی به جای گذرواژه نیز توصیه می‌شود.

٦- اعمال سیاست استفاده از گذرواژه‌های پیچیده

گذرواژه‌های ضعیف و رایج به آسانی از طریق حملات سعی و خطا[٤] لو می‌روند. سازمان می‌بایست سیاست‌های امنیتی مناسبی را اتخاذ کند. لزوم تخصیص گذرواژه پیچیده، عدم استفاده مجدد از گذرواژه‌های تکراری و قفل شدن نام کاربری در صورت ورود گذرواژه نادرست از جمله این سیاست‌هاست که می‌بایست مدنظر قرار داده شود.

با استفاده از pam_cracklib در تنظیمات ماژول PAM می‌توان کاربران را ملزم به استفاده از گذرواژه‌های پیچیده کرد. برای این منظور باید مراحل زیر دنبال شود:

الف) برای باز کردن فایل تنظیمات PAM فرمان زیر اجرا شود:

```
sudo nano /etc/pam.d/system-auth
```

ب) عبارت زیر به فایل افزوده شود:

```
/lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-2 dcredit=-2
```

با افزوده شدن عبارت فوق تنها گذرواژه‌های با حداقل طول ۸ نویسه که شامل حروف بزرگ و کوچک و عدد نیز باشد قابل قبول خواهد بود.

۷- به‌روزرسانی هسته و نرم‌افزارهای نصب شده

یکی از نکات مهم در نگهداری سرورهای Linux، نصب اصلاحیه‌ها است. در Linux ابزارهایی برای به‌روزرسانی بسته‌های نصب شده و ارتقای نسخه سیستم عامل وجود دارد که نمونه‌هایی از آن بشرح زیر است:

`sudo yum update`	در توزیع‌های Redhat
`sudo apt-get update && apt-get upgrade`	در توزیع‌های Debian

۸- فعال کردن SELinux

SELinux[٥] یکی از پراستفاده‌ترین ماژول‌های امنیتی سیستم عامل Linux است که روش‌های کنترل دسترسی را ارائه می‌کند.

۹- استفاده از دیواره آتش

از دیواره آتش و حتی‌الامکان نفوذیاب استفاده شده و بغیر از ترافیک مجاز سایر ارتباطات مسدود شود.

---

[٤] Brute Force

[٥] Security-Enhanced Linux

۱۰- جداسازی پارتیشن‌های هارد دیسک

توصیه می‌شود مسیرهای سیستمی زیر هر کدام در یک پارتیشن مجزا قرار گیرند:

- /usr
- /home
- /var and /var/tmp
- /tmp

۱۱- بررسی منظم سوابق رویدادهای سیستم

مسیر پیش‌فرض فایل‌های حاوی سوابق رویدادها[۶] بشرح زیر است:

- /var/log/message – تمامی سوابق رویدادها
- /var/log/auth.log یا /var/log/secure – سوابق رویدادهای اصالت‌سنجی[۷]
- /var/log/kern.log – سوابق رویدادهای مربوط به هسته سیستم عامل
- /var/log/cron.log – سوابق رویدادهای مربوط به زمانبندی اجرای فرامین
- /var/log/boot.log – سوابق رویدادهای راه‌اندازی سیستم
- /var/log/utmp یا /var/log/wtmp – سوابق رویدادهای ورود به سیستم

مرور دوره‌ای و منظم موارد مذکور توصیه می‌شود.

۱۲- حذف واسط گرافیکی

بر روی سرورهای مبتنی بر سیستم عامل Linux غیرفعال نمودن واسط گرافیکی[۸] و استفاده از واسط خط فرمان[۹] بجای آن توصیه می‌شود.

۱۳- نصب نرم‌افزار Rootkit Hunter

برای مقابله با بدافزارهای پیشرفته Rootkit بکارگیری ابزارهایی همچون Rootkit Hunter (rkhunter) توصیه می‌شود.

۱۴- مسدود نمودن دسترسی نام‌های کاربری با گذرواژه تهی

با اجرای فرمان زیر می‌توان به فهرست کاربران با گذرواژه تهی[۱۰] دست پیدا کرد:

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

توصیه می‌شود دسترسی کاربران مذکور به سیستم با اجرای فرمان زیر مسدود شود:

```
sudo passwd -l <accountName>
```

---

۶ Log Files
۷ Authentication
۸ Graphical User Interface
۹ Command Line Interface
۱۰ Blank

۱۵- بررسی درگاه‌های باز

درگاه‌های در وضعیت شنود[۱۱] بررسی شده و در صورت عدم نیاز غیرفعال شوند.

با اجرای یکی از فرامین زیر می‌توان فهرست درگاه‌های باز شبکه را مشاهده کرد:

```
netstat -tulpn
ss -tulpn
```

۱۶- رمزنگاری دیسک

توصیه می‌گردد با بکارگیری ابزارهایی همچون LUKS[۱۲] دیسک دستگاه‌های قابل حمل رمزگذاری شود.

۱۷- رمزنگاری فایل‌ها با استفاده از ابزار GPG

با بکارگیری ابزارهایی همچون GPG، رمزگذای فایل‌های حاوی داده‌های حساس و بااهمیت توصیه می‌گردد.

۱۸- غیرفعال کردن IPv6

در صورت عدم استفاده از نشانی IPv6، غیرفعالسازی آن توصیه می‌شود.

۱۹- حذف دسترسی نوشتن از روی مسیر /boot

هسته اصلی سیستم عامل Linux و سایر فایل‌های مرتبط با آن در مسیر /boot قرار دارند؛ با حذف دسترسی نوشتن (فقط خواندنی) می‌توان از دسترسی‌های غیر مجاز را مسدود کرده و از تغییر فایل‌های مهم در این مسیر جلوگیری کرد.

برای این منظور، باید مراحل زیر دنبال شود:

الف) با اجرای فرمان زیر فایل fstab اجرا شود:

```
sudo nano /etc/fstab
```

ب) عبارت زیر به انتهای فایل fstab افزوده شود:

```
LABEL=/boot     /boot     ext2     defaults,ro     1 2
```

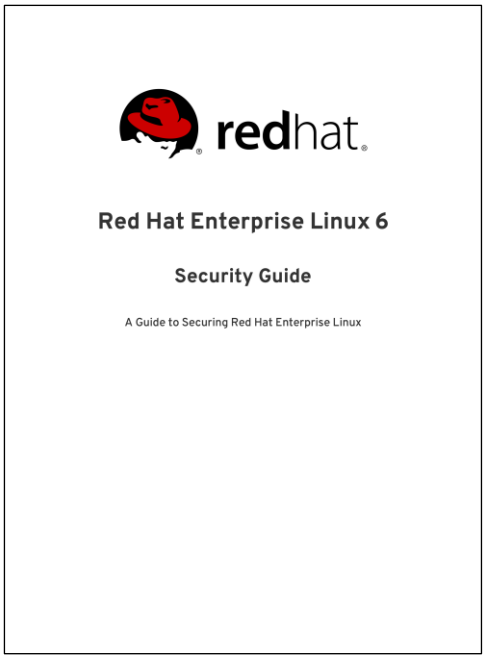
برای اعمال تغییرات لازم است یک بار سیستم راه‌اندازی مجدد[۱۳] شود.

---

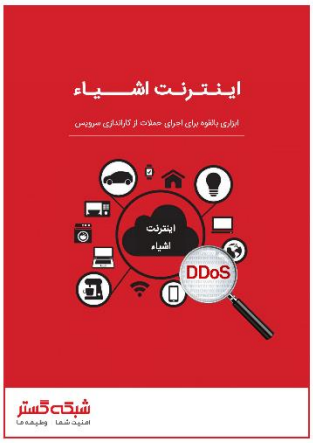
[۱۱] Listening
[۱۲] Linux Unified Key Setup
[۱۳] Restart

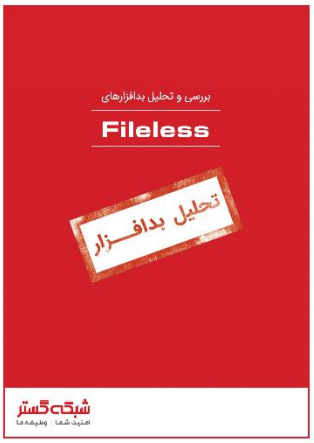
۲۰- نصب ضدبدافزار

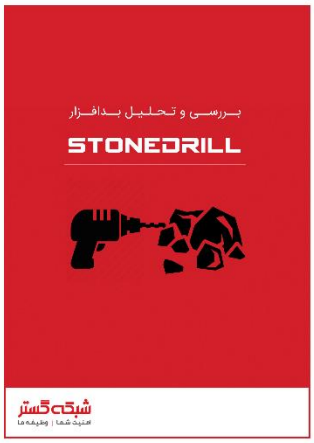
از ضدویروس به‌روز و قدرتمند استفاده شود. برای این منظور می‌توانید از نرم‌افزارهای سازمانی McAfee Endpoint Security for Linux یا Bitdefender Endpoint Security Tools for Linux اضافه کرد.

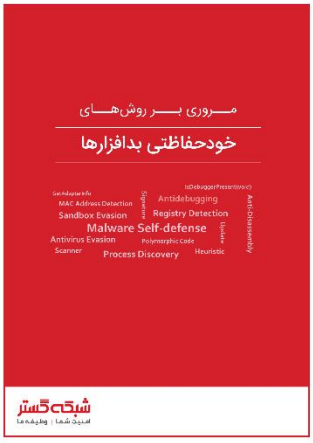


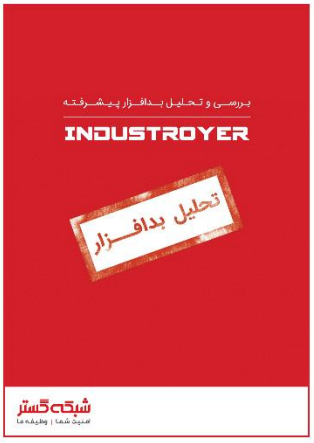
در اتاق خبر شبکه گستر بخوانید...

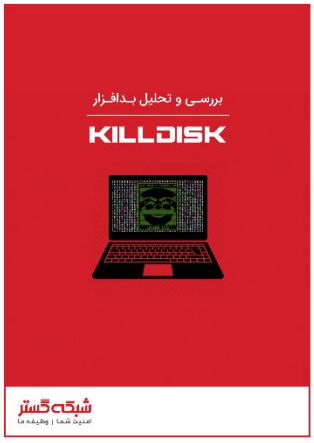


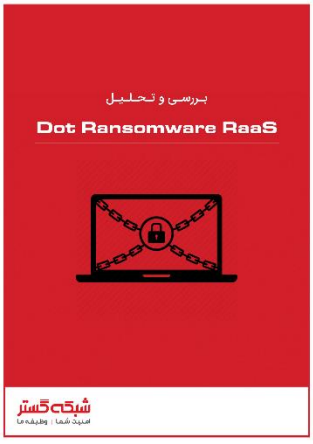


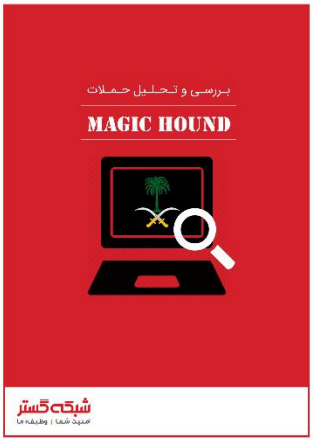


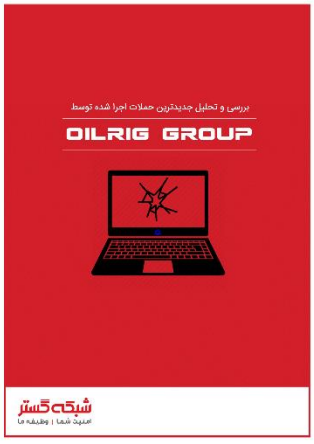












شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

اتـــاق خـبـــر

newsroom.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

تارنمای شـرکت

www.shabakeh.net

شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

info@shabakeh.net www.shabakeh.net