مستندات مربوط به پیاده سازی عملی

ضبط شده برای این پروژه: ۹

زیرنویس شده: ۲

به زبان فارسی: ۱۲

مجموع: ۲۳

S3T2

در مورد پارامترهای کرنل که در فایل /etc/sysctl.conf قابل افزودن هستند صحبت شد.

دستورات شامل :

- بررسی لیست پارامترهای اعمال شده و فعال
- اپلای کردن تغییرات انجام شده در فایل sysctl
- نمایش چند نمونه از پارامترهای کاربردی
- تست و انجام اثبات به منظور نادیده گرفتن درخواست های اکوی پینگ

در هر دو سیستم عامل انجام گرفته شد و در مورد بازگشت و حذف یک پارامتر خاص هم صحبت شد.

- https://www.youtube.com/watch?v=0QgUPK24NNE&t=605s

در این ویدیوی فارسی هم در مورد یک سری پارامترهای امن سازی برای وب سرور ها صحبت شده و نمونه پارامترها از سایت ایشان قابل دسترسی هست:

- https://linuxacademy.ir/?p=11710

بریده مربوط به بخش پارامترهای کرنل از ویدیوی فوق هم به مستندات افزوده شد.

S3T3

در مورد برنامه AppArmor صحبت شد. به شکل پیشفرض روی ابونتو نصب هست.

- با دستور aa-status مشاهده می شود که اپ آرمور در حال حاضر چه فعالیت هایی دارد
- با دستور systemctl status apparmor میشه وضعیت فعلی سرویس رو مشاهده کرد و با پارامتر های enable یا start اون رو فعال کرد یا با disable و stop اون رو غیرفعال کرد
- تفاوت با SELinux که جزئی از خود لینوکس هست اما اپ آرمور یک سرویس هست، و این دو همزمان نمیتونن با همدیگه اجرا بشن
- سه تا مودی که aa-status نمایش میده تشریح شد:
  - حالت enforce: یعنی اعمال اجباری کاری که برای اون پروفایل تعریف شده
  - حالت complain: یعنی اگه پروفایل هایی که در این بخش تعریف شدن بخوان کاری بجز چیزی که بهشون مجوز داده شده رو انجام بدن، قادر به انجامش هستن اما قبلش اخطار و اطلاعیه دریافت می کنن
  - و حالت سومی که اگه پروفایل در اون زیرمجموعه باشه، لاگ گیری یا محدودیتی روی اون اعمال نمیشه
- حالا که می دونیم چطور apparmor رو چک کنیم، به سراغ تعریف یک policy برای سرویسی که داریم می رویم. مثلا یک اسکریپت داریم هر بار در استارت آپ اجرا میشه. حالا براش یک پروفایل ایجاد می کنیم تا بتونیم تحت اپ آرمور اون رو مدیریت کنیم
- اینکارو با دستور aa-genprof انجام می دیم که نیازمند این هست اول پکیج apparmor-utils نصب بشه
- با دستور aa-logprof لاگ هارو بررسی می کنه و اگه اسکریپت به دسترسی های بیشتری نیاز داشته باشه اونها رو بهش اعطا میکنه که برنامه ها و اسکریپت ها در اثر نیاز به دسترسی بیشتر بخاطر آپدیت شدن یا ... از کار نیافتن
- همچنین لازمه که بعد از ساختن پروفایل یکبار برنامه اجرا بشه و اگه به ارور خورد دستور بالا انجام بشه تا زمانی که دیگه اروری مشاهده نشه و اپ آرمور دسترسی های لازم رو بفهمه و بهش بده
- https://youtube.com/watch?v=0t-UZFBNyF0

S3T4

- https://youtube.com/watch?v=ZhMw53Ud2tY

بخش شماره ۱ ویدیو، راهنمایی در مورد آپدیت دستی به شکل apt dist-upgrade و نصب برنامه ای برای بروزرسانی و آپگرید خودکار سرور لینوکسی. بخش اول ویدیوی فوق همچنین زیرنویس شد و داخل مستندات وارد شد.

S3T5

در رابطه با اسکن و چکاپ فوری سیستم عامل و سرویس های آن از لحاظ امنیتی توضیح داده شد. ابزار مورد استفاده Lynis است. اسکن جامع با یک دستور نمایش داده شد و نتایج خروجی به شکل ابتدایی تحلیل شدند.

S4T1

دسترسی ها(Permission) و مالکیت فایل:

دو ویدیوی فارسی از جادی در این مورد به مستندات افزوده شد که به شکل کامل مباحث مربوط به دسترسی ها و گروه های کاربری و گروه مالک را نسبت به فایل و دایرکتوری ها توضیح میدهد.

ویدیو ها مطابق ماژول 104.5 دوره LPIC-1 و در دو قسمت ضبط شده.

- https://youtu.be/CEW_ozeLeK0?si=WXTLIbOTOgKLslY7
- https://youtu.be/q9UZ4LhfLvI?si=8V6Wjlt0epTXekOo
- https://wiki.archlinux.org/title/File_permissions_and_attributes

S5T1

یک ویدیوی پایه در مورد کار با iptables و چگونگی پیکربندی و امن سازی پروتکل ICMP با استفاده از آن، بلاک کردن درخواست ها از منابع تعریف نشده و پاسخ دادن تنها به یک آی پی از پیش تعریف شده.

یک ویدیوی کامل به زبان فارسی و آموزش iptables از سطح مقدماتی در مستندات پیوست شد:

- https://www.youtube.com/watch?v=JMHDo4X7v1s
- https://linuxacademy.ir/ip-tables/

S5T2

درمورد سرویس KnockD و مزایای امنیتی استفاده از آن، یک ویدیوی با زبان فارسی در مستندات پیوست شد. این سرویس به عنوان یک مکمل امنیتی برای سرویس های تحت وب سرور می باشد. با کمک این ابزار می توان پورت نامبر خاصی را به صورت ریموت، فعال یا غیرفعال کرد. به طور مثال با ارسال مجموعه ای از دستورات به همراه کلید از پیش تعریف شده به سمت سرور، پورت ۲۲ برای SSH در فایروال باز می شود تا ما دسترسی موقتی جهت اتصال داشته باشیم. سپس وقتی کار تمام شد، با ارسال دستور مشخصی اقدام به بازگردانی پورت مربوطه به لیست مسدود ها می کنیم:

- https://youtube.com/watch?v=WhPHKvNUpAw

S5T3

درباره غیرفعالسازی سرویس های غیرضروری روی سیستم و سرور، به شکل سیستمی و سرویسی صحبت شد. در مورد لزوم غیرفعالسازی ریشه ای آنها و minimize کردن سرویس های فعال به خصوص سرویس ها با دسترسی وب، به جهت کاهش تهدیدات امنیتی و در امان ماندن از تهدیدات روز صفر (zero-day attacks)

برای نمایش ویدیویی، سرویس SSH روی سرور Ubuntu به طور ریشه ای متوقف و غیرفعال شد و دسترسی تنها از طریق کنسول میسر بود. تاکید شد که این متد با غیرفعالسازی از طریق فایروال یا متد های دیگر دارای تفاوت است.

یک ویدیوی کوتاه به زبان فارسی در مورد دستور autoremove هم به مستندات افزوده شد:

- https://youtu.be/0QgUPK24NNE?si=znhTupmVlKlirMcL&t=863

S5T4

در مورد تغییر پورت SSH، غیرفعالسازی دسترسی کاربر root برای لاگین با SSH و مواردی که در ویدیوهای آتی صحبت خواهد شد، توضیح داده شد.

ویدیویی به زبان فارسی در مورد امن سازی مقدماتی SSH و برخی دیگر از پارامترهای درون فایل کانفیگ SSH به مستندات افزوده شد:

- https://youtu.be/0QgUPK24NNE?si=4_lTRANTnvOcLIAf&t=909

S5T6

درباره اهمیت توجه به امن سازی IPv6 روی سرور، نحوه غیرفعالسازی آن از روش ماژول های کرنل و اجباری کردن IPv4 برای سرویس SSH صحبت شد.

S6T1

یک ویدیوی مقدماتی در رابطه با ساخت و آپلود کلید SSH از سمت کلاینت به سمت سرور در مستندات قرار داده شد، همینطور روش کپی دستی محتویات کلید و قراردادن آن در فایل کلید های مجاز در مسیر home یوزر مربوطه توضیح داده شد. در این فایل همچنین در مورد یکی بودن owner فایل حاوی کلید خصوصی با یوزری که قصد اتصال را دارد صحبت شده:

- https://youtu.be/vu53J6wyOII?si=wItecyM7gHmZhaCi&t=758

S6T2

ویدیوی فارسی که به طور کامل در خصوص نصب و پیکربندی پکیج libpam مربوط به گوگل به منظور فعالسازی ورود دومرحله ای توضیح داده و چگونگی کار را نمایش می دهد:

- https://youtu.be/f-lw-w3cXeA?si=8aQ5Gyo9kqLOFUvW

S6T3

توضیح مقدماتی در مورد Fail2ban:

- https://youtu.be/0QgUPK24NNE?si=RQE9ecRdtYI-vGX_&t=1253

آموزش عملی و یک مقاله از شرکت ابرزس در مورد بکارگیری از این ابزار:

- https://xaas.ir/blog/fail2ban-2/
- https://xaas.ir/blog/fail2ban/

هر دو ویدیو ها در مستندات قرار گرفته اند.

S8T1

این تاپیک که به اعمال سیاست های مرتبط با کلمه عبور(پسورد) می پردازد، به شکل عملی پیاده سازی و کپچر شد. در پیاده سازی از ماژول libpam-pwquality استفاده شد و از مرجع آنلاین زیر برای توضیح پارامتر های فایل کانفیگ ماژول استفاده شد:

- https://linux.die.net/man/8/pam_pwquality

S8T3

ابزار auditd به شکل عملی مورد پیاده سازی و بررسی قرار گرفت. از یک نشست جداگانه به سرور وارد شدیم و به شکل زنده تغییراتی که در فایل لاگ ها نوشته می شد را مانیتور کردیم.

S8T6

ویدیوی فارسی زیر در مستندات قرار گرفت. در آن به اهمیت و دسترسی های بالای کاربر root اشاره شده و در این مورد صحبت شد که بهتر است با یوزر به غیر از root در سرور لاگین کرده و کاربر را عضو گروه sudo کنیم تا در زمان اجرای دستورات حساس و غیرقابل بازگشت، یک مرحله امنیت ایجاد کرده باشیم.

- https://www.youtube.com/watch?v=O1N8q9zSwsE

S9T3

برای پیاده سازی عملی، از پکیج timeshift استفاده شد و توضیحات لازم در مورد چگونگی ایجاد بکاپ، مشاهده لیست بکاپ ها، ریستور کردن یک بکاپ موجود در لیست و پاکسازی یا حذف یک بکاپ از لیست به منظور آزادسازی فضای دیسک ارائه شد.