دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

مبانی رایانش امن

تکلیف سوم

دستیار آموزشی

داراب زندیه
علیرضا آرامی مهر

استاد

دکتر مجتبی خلیلی

زمان تحویل

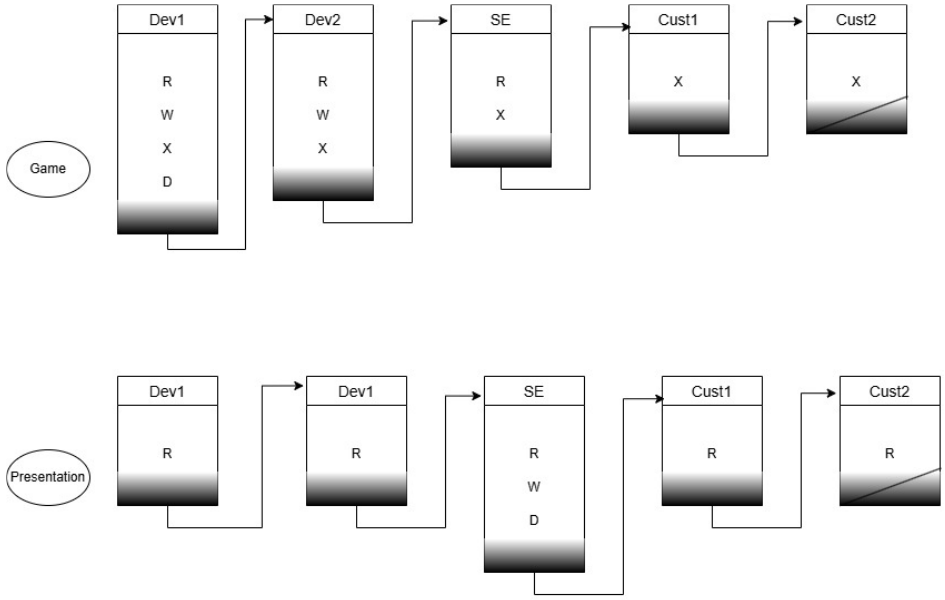
1404/04/04

نکات تحویل تکلیف

- فایل‌های خود را با فرم `PHW1_Name1_StudentNum1_Name2_StudentNum1.zip` ارسال کنید. توجه شود که به فایل‌هایی که نام‌گذاری آنها به‌صورت فرمت گفته‌شده نباشد، نمره‌ای تعلق نخواهد گرفت.
- پاسخ‌های شما باید به‌صورت تایپ‌شده باشد، به پاسخ‌های دست‌نویس نمره‌ای تعلق نخواهد گرفت.
- به پاسخ‌های بدون توضیح امتیاز و نمره‌ای تعلق نخواهد گرفت.
- در صورت وجود هرگونه ابهام می‌توانید از طریق تلگرام سؤالات خود را با دستیار آموزشی مربوط به این تکلیف مطرح کنید. آیدی تلگرام دستیارهای آموزشی مربوط به این تکلیف: @dzshb و @A__Aramimehr
- در صورت وجود شباهت واضح، نمره‌ای به پاسخ تعلق نمی‌گیرد.
- پاسخ تکلیف را حتماً در سامانه یکتا آپلود کنید و از ارسال تکلیف به ایمیل یا تلگرام اکیداً خودداری کنید.
- **مشارکت گروهی:** همه اعضای گروه باید مشارکت کنند (مثلاً در کدنویسی، تحلیل، آماده‌سازی ویدئو).
- **کد و ابزارها:** تمام کدهای منبع، دستورات یا ابزارهای استفاده‌شده را با توضیحات مختصر یا شرح عملکردشان ارائه دهید.
- **توضیحات ویدیویی:** برای هر سوال، یک ویدئو ارائه دهید که راه‌حل را توضیح داده و نتایج را نشان دهد. ویدئو را با شماره سوال به وضوح برچسب‌گذاری کنید.
- **گزارش:** برای هر سوال عملی یک گزارش کتبی ارائه دهید که شامل:
  - پاسخ به تمام بخش‌های سوال.
  - تصاویر، عکس‌ها یا نمایش‌های بصری در صورت درخواست.
  - توضیحات و تحلیل‌ها طبق مشخصات.

۱ سوالات تئوری

شما مدیر یک محصول فنی هستید و باید سطح دسترسی توسعه‌دهندگان ،(Developers) مسئول فروش (Sales Engineer) و مشتریان (Customers) را تعریف و مشخص کنید. با توجه به ACL داده‌شده، به سوالات زیر پاسخ دهید:



شکل ۱: نمودار ACL

سوال ۱

استفاده این مدیر از Access Control Policies به کدام نوع سیاست شباهت دارد؟ دلیل خود را توضیح دهید.

سوال ۲

با توجه به ACL داده‌شده، یک Capability List رسم کنید.

سوال ۳

با توجه به ACL داده‌شده، برای سه نقشِ «توسعه‌دهنده»، «مسئول فروش» و «مشتری» یک Access Matrix طراحی و رسم کنید.

سوال ۴

Access Control List چیست؟ توضیح دهید.

سوال ۵

تفاوت دستورات chmod، chown، setfacl و getfacl چیست؟ توضیح دهید.

۲ سوالات عملی

سوال ۱

مدیر پروژه تیمی متشکل از دو توسعه‌دهنده و یک مسئول فروش دارد و پروژه را به دو مشتری ارائه می‌دهد. پروژه شامل دو فایل است:

- فایل1/opt/project/dev/Game/
- فایل2/opt/project/presentation/

مراحل اجرا

- ایجاد کاربران:
  - دو کاربر با نقشِ «توسعه‌دهنده»
  - یک کاربر با نقشِ «مسئول فروش»
  - دو کاربر با نقشِ «مشتری»
- تنظیم مجوزها مطابق ACL زیر:
  - الف) همه توسعه‌دهندگان: دسترسی کامل (read, write, execute)
  - ب) یکی از توسعه‌دهندگان: علاوه بر مجوز کامل، توانایی حذف فایل (unlink) نیز داشته باشد
  - ج) مسئول فروش: تنها مجوز خواندن (r) و اجرای (x) فایلِ Game
  - د) مشتریان: فقط مجوز اجرای (x) فایلِ Game داشته باشند

نکته

منظور از «دسترسی کامل» برای توسعه‌دهندگان همان مجوزهای rwx در لینوکس است.

در رسم Capability List و Access Matrix، نام کاربران و نقش‌های مربوطه را بنویسید و مجوزهای دقیق (r, w, x) را برای هر فایل مشخص کنید.

سوال ۲

در دنیای امنیت password list یا wordlist ها فایل‌هایی هستند که شامل مجموعه‌هایی از کلمات و یا رمزعبورها هستند و برای کرک کردن یا حملات brute force مورد استفاده قرار می‌گیرند. یکی از معروف‌ترین این wordlist ها rockyou می‌باشد؛ در سال ۲۰۰۹ تمامی پسوردهای کاربران یک برنامه اجتماعی (در حدود ۳۲ میلیون اکانت) به نام RockYou هک شد و به بیرون درز پیدا کرد، پس از گردآوری و تجمیع آن در فایلی به نام rockyou.txt منجر به این شد تا یکی از معروف‌ترین و پرکاربردترین wordlist ها بوجود بیاید.

نحوه دانلود و استفاده از این wordlist

در صورتی که از سیستم عامل Kali Linux استفاده می‌کنید این فایل به صورت فشرده شده در مسیر مشخص شده قابل مشاهده است.

```
┌──(darab㉿kali)-[~]
└─$ ls -lhrt /usr/share/wordlists
total 51M
-rw-r--r-- 1 root root 51M May 12  2023 rockyou.txt.gz
lrwxrwxrwx 1 root root  26 Feb 26 15:57 amass -> /usr/share/amass/wordlists
lrwxrwxrwx 1 root root  37 Feb 26 15:57 wifite.txt -> /usr/share/dict/wordlist-probable.txt
lrwxrwxrwx 1 root root  30 Feb 26 15:57 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root  25 Feb 26 15:57 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root  35 Feb 26 15:57 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root  45 Feb 26 15:57 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root  28 Feb 26 15:57 john.lst -> /usr/share/john/password.lst
lrwxrwxrwx 1 root root  27 Feb 26 15:57 legion -> /usr/share/legion/wordlists
lrwxrwxrwx 1 root root  46 Feb 26 15:57 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root  41 Feb 26 15:57 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
lrwxrwxrwx 1 root root  41 Feb 26 15:57 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root  25 Feb 26 15:57 wfuzz -> /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root  39 Feb 26 15:57 sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
```

شکل ۲: مسیر فایل rockyou

```
┌──(darab㉿kali)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz

┌──(darab㉿kali)-[/usr/share/wordlists]
└─$ ls -lhrt
total 134M
-rw-r--r-- 1 root root 134M May 12  2023 rockyou.txt
lrwxrwxrwx 1 root root   26 Feb 26 15:57 amass -> /usr/share/amass/wordlists
lrwxrwxrwx 1 root root   37 Feb 26 15:57 wifite.txt -> /usr/share/dict/wordlist-probable.txt
lrwxrwxrwx 1 root root   30 Feb 26 15:57 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root   25 Feb 26 15:57 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root   35 Feb 26 15:57 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root   45 Feb 26 15:57 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root   28 Feb 26 15:57 john.lst -> /usr/share/john/password.lst
lrwxrwxrwx 1 root root   27 Feb 26 15:57 legion -> /usr/share/legion/wordlists
lrwxrwxrwx 1 root root   46 Feb 26 15:57 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root   41 Feb 26 15:57 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
lrwxrwxrwx 1 root root   41 Feb 26 15:57 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root   25 Feb 26 15:57 wfuzz -> /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root   39 Feb 26 15:57 sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt

┌──(darab㉿kali)-[/usr/share/wordlists]
└─$ cat rockyou.txt | wc -l
14344392
```

شکل ۳: دستور استخراج کردن

پس از اجرای دستور نمایش داده شده فایل txt این wordlist با حجم ۱۳۴ مگابایت باید extract شده باشد، همچنین در این فایل در حدود ۳.۱۴ میلیون پسورد متمایز وجود دارد.

اگر از توزیع‌های لینوکسی غیرامنیتی نظیر ubuntu استفاده می‌کنید، می‌توانید این wordlist را به صورت فشرده

شده یا txt از این ریپازیتوری (https://github.com/brannondorsey/naive-hashcat/releases/) دانلود کنید.

الف)

وظیفه PAM (Pluggable Authentication Module) در سیستم‌های لینوکسی چیست؟ همچنین ساختار کلی این ماژول را شرح دهید.

ب)

فایل مربوط به تنظیمات و قوانین پسوردها که در این ماژول قرار دارد را پیدا کنید و آن را به نحوی تغییر دهید که شروط زیر برای پسوردهای جدید در نظر گرفته شود:

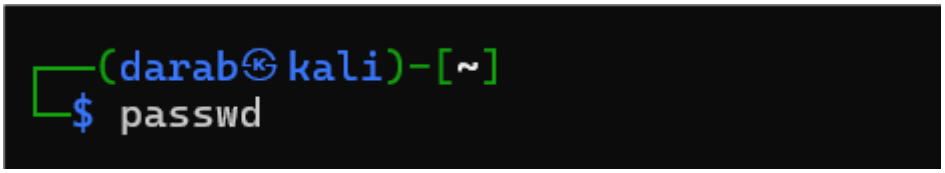
- طول پسورد انتخابی باید حداقل ۵ کاراکتر باشد.
- پسورد باید حداقل شامل یک کاراکتر خاص، یک حرف بزرگ و کوچک انگلیسی و یک عدد باشد.
- پسورد نباید برابر با نام کاربری یا بخشی از آن باشد.

همچنین درصورتی که تابع هش بکار رفته برای هش کردن پسورد در این فایل برابر با sha512 نمی‌باشد، آن را به این تابع هش تغییر دهید (تابع هش پیش‌فرض در اکثر توزیع‌های لینوکسی yescrypt می‌باشد).

در پایان، انتهای خط مربوط به تغییرات اعمال‌شده در این ماژول dictcheck=0 را اضافه کنید.

پ)

حال با اجرای دستور زیر در اکانت اصلی خود (اکانت غیر روت)، پسورد خود را به Saturday1! تغییر دهید. همچنین می‌توانید یک کاربر جدید با این پسورد بسازید.



شکل ۴: نمودار تغییرات تعداد CD4+ در طول زمان در شبیه‌سازی

سپس با نمایش مقدار ذخیره شده هش پسورد این کاربر که تغییر کرده است، بخش‌های مختلف آن را مشخص و توضیح دهید.

ج)

به کمک یکی از ابزارهای john یا hashcat و پسورد لیست rockyou این هش را کرک کنید و مقدار اولیه آن را بیابید.

نکته

در پایان تغییرات اعمال‌شده را به لحاظ امنیتی به حالت اولیه خود بازگردانید و پسورد خود را عوض کنید.