CTF сорилгын тайлбар: Zip нууц үг эвдэх ба LSB нууцлал

Энэхүү тайлбарт нууц үгээр хамгаалагдсан zip файлыг эвдэх, мөн зураг дотор LSB нууцлалаар нуусан флагийг олох CTF (Capture The Flag) сорилгыг хэрхэн шийдвэрлэсэн алхмуудыг дэлгэрэнгүй тайлбарласан болно.
Сорилгыг зохиогч: Luci4

Сорилгын тойм

Сорилгод хоёр файл өгсөн: нууц үгээр хамгаалагдсан zip архив (challenge.zip) болон энгийн мэт харагдах зураг файл (mystery.png). Зорилго нь эдгээр файлуудад нуугдсан флагийг олох байв.

Алхам 1: Эхний анализ ба Zip файлыг тодорхойлох

Файлуудыг хүлээн авсны дараа эхний алхам нь тэдгээрийн төрлийг тодорхойлох явдал юм. Үүний тулд Linux систем дээр file командыг ашиглах нь тохиромжтой:
file challenge.zip mystery.png

Энэ команд нь challenge.zip нь zip архив, харин mystery.png нь PNG зураг болохыг баталгаажуулна. challenge.zip-ийн агуулгыг задлах оролдлого хийхэд нууц үгээр хамгаалагдсан болох нь харагдана.
unzip challenge.zip

Энэ команд нь нууц үг оруулахыг шаардах бөгөөд бидэнд нууц үг байхгүй байна.

Алхам 2: Zip нууц үгийг хүчээр эвдэх (Brute-forcing)

Zip файл нь нууц үгээр хамгаалагдсан бөгөөд CTF сорилгод сул эсвэл түгээмэл нууц үг ашиглах нь элбэг байдаг тул rockyou.txt толь бичиг нь хүчээр эвдэх халдлагад тохиромжтой сонголт юм. rockyou.txt нь түгээмэл хэрэглэгддэг нууц үгүүдийг агуулсан том үгийн жагсаалт юм.
Zip нууц үг эвдэхэд хэд хэдэн хэрэгсэл ашиглаж болно. fcrackzip нь энэ зорилгоор түгээмэл хэрэглэгддэг командын мөрний хэрэгсэл юм.
fcrackzip -u -D -p rockyou.txt challenge.zip

- -u: Эвдсэн нууц үгээр файлыг задлах оролдлого хийнэ.
- -D: Халдлагад толь бичгийн файл ашиглана.
- -p rockyou.txt: Толь бичгийн файлын замыг заана.

Өөрөөр хэлбэл, john the ripper-ийг zip2john хэрэгсэлтэй хамт ашиглаж болно. Эхлээд zip

файлыг john-д ойлгогдох hash формат руу хөрвүүлнэ:
zip2john challenge.zip > challenge.hash
john --wordlist=rockyou.txt challenge.hash

Хүчээр эвдэх хэрэгслийг ажиллуулсны дараа, хэрэв нууц үг rockyou.txt-д байвал, хэрэгсэл эвдсэн нууц үгийг гаргаж ирнэ. Нууц үг нь password123 байсан гэж үзье.

Алхам 3: Zip файлын агуулгыг задлах

Одоо нууц үгийг мэдсэн тул zip файлын агуулгыг задлах боломжтой:
unzip challenge.zip

Нууц үг оруулахыг шаардахад, эвдсэн нууц үгийг (password123) оруулна. Энэ нь zip архив доторх файлуудыг задлана. Задарсан файл нь өөр зураг байсан гэж үзье, жишээлбэл hidden_image.png гэсэн нэртэй.

Алхам 4: Задарсан зургийг нууцлалын хувьд шинжлэх

Одоо сорилго нь задарсан зураг руу (hidden_image.png) шилжлээ. Сорилго нь криминалистиктэй холбоотой тул нууцлал (өгөгдлийг бусад өгөгдөл дотор нуух урлаг) нь ашиглагдсан байх магадлалтай арга юм. Хамгийн бага ач холбогдолтой бит (LSB) нууцлал нь зургийн пикселийн өгөгдлийн хамгийн бага ач холбогдолтой битүүдэд өгөгдлийг нуудаг түгээмэл арга юм.
Сорилгын санууллгад улаан суваг болон 0, 1, 2, 3-р битүүдийг тодорхой дурдсан. Энэ нь LSB нууцлалыг улаан өнгөний сувгийн доод битүүдэд төвлөрүүлсэн болохыг хүчтэй илтгэж байна.

Алхам 5: LSB нууцлал ашиглан өгөгдөл гаргаж авах

zsteg зэрэг хэрэгслүүд нь LSB зэрэг төрөл бүрийн нууцлалын аргаар нуусан өгөгдлийг илрүүлэх, гаргаж авахад маш сайн. zsteg нь зургийг шинжилж, боломжит нуугдсан өгөгдлийн урсгалыг мэдээлдэг.
zsteg hidden_image.png
```zsteg` нь өөр өөр битийн хавтгай болон өнгөний сувгуудыг шинжилнэ. Улаан сувагт, ялангуяа 0, 1, 2, 3-р битүүдэд өгөгдөл олдсон болохыг заасан гаралтыг хайна уу. Гаралт нь гаргаж авсан стрингүүд эсвэл флаг форматтай төстэй өгөгдлийг (жишээлбэл, `flag{...}`) харуулж болно.

Хэрэв `zsteg` флагийг шууд илрүүлэхгүй боловч заасан битийн хавтгайнуудад өгөгдөл байгааг илтгэвэл, та эдгээр хавтгайнуудаас түүхий өгөгдлийг гаргаж авахын тулд `zsteg`-ийг тодорхой сонголтуудтай хамт ашиглах шаардлагатай байж болно:
```

```bash
zsteg -E 'b0,b1,b2,b3,r' hidden_image.png > extracted_data.bin
```

- -E: Өгөгдөл гаргаж авна.
- 'b0,b1,b2,b3,r': Улаан сувгийн (r) 0, 1, 2, 3-р битүүдээс гаргаж авахыг заана.

extracted_data.bin файлыг шалгана уу. Энэ нь флагийг шууд агуулсан байж болох эсвэл цаашдын анализ шаардлагатай байж болно (жишээлбэл, хэрэв энэ нь өөр нуугдсан файл байвал нийтлэг файлын толгойг шалгах).

StegSolve ашиглах өөр нэг сонголт:

StegSolve нь зураг дээрх нууцлалыг шинжлэхэд зориулагдсан график хэрэглэгчийн интерфэйстэй (GUI) маш хүчирхэг хэрэгсэл юм. StegSolve-ийг ашиглахын тулд:

1. StegSolve.jar файлыг татаж аваад ажиллуулна уу (Java орчин шаардлагатай).
2. "File" -> "Open" дарж hidden_image.png файлыг нээнэ.
3. "Analyse" цэснээс "Data Extract" эсвэл "Bit Planes" сонголтуудыг ашиглана.
4. Улаан сувгийг сонгож, 0, 1, 2, 3-р битүүдийг идэвхжүүлнэ.
5. Өөр өөр хослолуудыг туршиж үзэх эсвэл гаргаж авсан өгөгдлийг харахын тулд "Preview" эсвэл "Save" дарна.

StegSolve нь өөр өөр битийн хавтгайнуудаас өгөгдлийг харах, хадгалах боломжийг олгодог бөгөөд энэ нь нуугдсан флагийг олоход тустай.

Алхам 6: Флагийг олох

Улаан сувгийн доод битүүдээс өгөгдлийг амжилттай гаргаж авсны дараа, флаг нь гаргаж авсан өгөгдөл дотор байх ёстой. Энэ нь энгийн текст стринг байж болох эсвэл сорилгын онцлогоос хамааран бага зэрэг декодлох шаардлагатай байж болно.

Ашигласан хэрэгслүүд

- file: Файлын төрлийг тодорхойлох.
- unzip: Zip архивыг задлах.
- fcrackzip эсвэл john the ripper ба zip2john: Zip нууц үгийг хүчээр эвдэх.
- zsteg: LSB нууцлалыг илрүүлэх, гаргаж авах.
- StegSolve: Зураг дээрх нууцлалыг шинжлэх график хэрэгсэл.
- (Заавал биш) Python ба Pillow: Өөрчлөн LSB гаргаж авах скрипт бичих.
- rockyou.txt: Хүчээр эвдэхэд ашигласан толь бичгийн файл.

Эдгээр алхмуудыг дагаснаар бид толь бичгийн халдлагаар zip нууц үгийг эвдэж, дараа нь улаан сувгийн заасан битийн хавтгайнуудад чиглэсэн LSB нууцлал ашиглан зурагнаас нуугдсан флагийг гаргаж авсан болно.