SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

IZVJEŠTAJ

LABORATORIJSKA VJEŽBA 1

BitLocker i dekripcija diska

Danica Majić

Split, lipanj 2022.

1. ZADATAK VJEŽBE

Kako bi zaštitili laptope, vanjske diskove, USB memorije od posljedica krađe, veoma često se upotrebljavaju tehnike enkripcije cijelih memorija. Jedna od tehnika zaštite podataka je korištenje BitLocker alata za šifriranje diska koje je dostupan u novijim verzijama Windowsa (Vista, 7, 8.1 i 10) Ultimate, Pro i Enterprise.

ZADATAK: Pretpostavite da ste dobili na analizu USB memoriju čiji je sadržaj enkriptiran korištenjem BitLockera. Nakon što ste napravili sigurnosnu kopiju USB memorije, vaš zadatak je saznati lozinku kojom je enkriptiran disk/USB.

2. POSTUPAK PROBIJANJA Bitlocker LOZINKE

Probijanje lozinke se sastoji od dva dijela: izvlačenje hash sadržaja iz sigurnosne kopije UBS-a koji je zaštićen lozinkom te stvarnog napada. Sačuvajte na računalu sliku USB-a koji se nalazi na OneDrive-u.

2.1 IZVLAČENJE HASH VRIJEDNOSTI – John the Ripper

Na računalu sačuvajte sigurnosnu kopiju USB-a koji je enkriptiran BitLockerom. Nakon toga, skinite verziju alata John the Ripper te ga raspakirajte. U nastavku izvucite hash korištenjem bitlocker2john alata korištenjem uputa u Terminalu/CMDu:

```
bitlocker2john -i imageEncrypted
Opening file /path/to/imageEncrypted
```

gdje je `imageEncrypted` sigurnosna kopija USB memorije. Trebali bi dobiti nešto slično u nastavku:

```
Signature found at 0x00010003
Version: 8
Invalid version, looking for a signature with valid version...

Signature found at 0x02110000
Version: 2 (Windows 7 or later)

VMK entry found at 0x021100d2
VMK encrypted with user password found!
VMK encrypted with AES-CCM

VMK entry found at 0x021101b2
VMK encrypted with Recovery key found!
VMK encrypted with AES-CCM

$bitlocker$0$16$a149a1c91be871e9783f51b59fd9db88$1048576$12$b0adb333606cd30103000000$60$c1633c8f7eb721ff42e3c29c3daea6da0189198af1516
$bitlocker$1$16$a149a1c91be871e9783f51b59fd9db88$1048576$12$b0adb333606cd30103000000$60$c1633c8f7eb721ff42e3c29c3daea6da0189198af1516
$bitlocker$2$16$2f8c9fbd1ed2c1f4f034824f418f270b$1048576$12$b0adb333606cd30106000000$60$8323c561e4ef83609aa9aa409ec5af460d784ce3f836e
$bitlocker$3$16$2f8c9fbd1ed2c1f4f034824f418f270b$1048576$12$b0adb333606cd30106000000$60$8323c561e4ef83609aa9aa409ec5af460d784ce3f836e
```

Kao što je prikazano u primjeru, bitlocker2john vraća 4 izlazna hasha s različitim prefiksom.

- Ako je uređaj šifriran metodom provjere autentičnosti korisničke lozinke, bitlocker2john ispisuje ta dva hasha:
  - $bitlocker$0$...: pokreće način brzog napada korisničke lozinke
  - $bitlocker$1$...: pokreće način napada korisničke lozinke s MAC provjerom (sporije izvršavanje, bez *false positives* rezultata)
- U svakom slučaju, bitlocker2john ispisuje sljedeća dva hasha:
  - $bitlocker$2$...: pokreće način brzog napada lozinke za oporavak
  - $bitlocker$3$...: pokreće način napada za oporavak lozinke s MAC provjerom (sporije izvršavanje, bez *false positives* rezultata)

Kopirajte hash koji počinje sa $bitlocker$1$...: te ga spremite u tekstualnu datoteku (npr. hash.txt). Navedena datoteka će se upotrebljavati za drugi alat kojeg ćemo opisati u nastavku - Hashcat.

2.2 PROBIJANJE LOZINKE – Hashcat

Skinite verziju alata Hashcat te ga raspakirajte. U nastavku ćemo koristiti naredbu za probijanje BitLocker lozinke korištenjem Hashcat alata iz Terminala/CMDa:

```
hashcat -m 22100 -a 3 hash.txt "xyz?d?d?d?d?d"
```

pri čemu -m 22100 predstavlja hash mode za BitLocker, xyz predstavlja **HINT** kojeg ćete dobiti od profesora, a ?d?d?d?d?d je niz od 5 brojeva koji hashcat mora pogoditi *bruteforce* napadom.

2.3 PODIZANJE SLIKE KOPIJE DISKA KORIŠTENJEM Arsenal Image Mounter ALATA

Na računalo sačuvajte Arsenal Image Mounter s kojom ćemo podigniti sigurnosnu kopiju USB-a u *Read-only modu*. Kada stisnete tipku Mount Image, pronađite sigurnosnu kopiju diska, označite Read only te Create "removable" disk device. Nakon toga bi se trebao pokazati BitLocker prozor upozorenja za unos lozinke. Kada unesete lozinku trebao bi se pojaviti sadržaj USB memorije.

3. RIJEŠENJE

Lozinka kojom je enkriptiran disk/USB je 21854671.