Zrozumienie BIOS-u

Ćwiczenie: Włamania do BIOS

cmospwd - program do odzyskiwania, przywracania i usuwania hasła CMOS/BIOS. Wykonując go na swojej/czyjejś maszynie możemy między innymi zapisać i odczytać (jako plain-text) jego hasło administracyjne do BIOS (o ile było ustawione i cmospwd był w stanie je odzyskać z pamięci CMOS)

W celu wykonania ćwiczenia wykonaj następujące kroki:

1. Jeśli nie korzystasz z Kali Linux, zainstaluj cmospwd (*szybsza opcja*).

   ```
   # Dla Ubuntu/Debian
   sudo apt-get install cmospwd
   # dla innych dystrybucji użyj yum/rpm/packman, zamiast apt
   ```

   Jeśli chcesz korzystać z Kali (*rekomendowana opcja*), cmospwd jest już w nim zainstalowany. Jeśli chcesz wiedzieć jak to zrobić, przejdź do sekcji **Stwórz własny Kali Linux Live USB** (poniżej)

2. Następnie zrestartuj komputer, wejdź do BIOS i ustaw hasło administratora i/lub tzw. hasło rozruchowe

3. Po ponownym zbootowaniu systemu wykonaj następujące komendy aby sprawdzić ustawione hasło:

   ```
   sudo cmospwd /w cmospwd_backup_file.bak # Write cmos_backup_file
   vim cmospwd_backup_file.bak # zobacz hasło do BIOS
   ```

4. Usuń hasło

   ```
   sudo cmospwd /k # resetowanie hasła BIOSu
   # możesz teraz zresetować komputer, aby sprawdzić, że hasło do BIOS zostało skasowane
   ```

5. Przywróć hasło z backupu

   ```
   sudo cmospwd /r cmospwd_backup_file.bak # Restore cmos_backup_file
   ```

6. Uwaga/Dodatkowe informacje dot. [włamań i obejścia haseł zapisanych w pamięci EPROM]

Stwórz własny Kali Linux Live USB

W tym celu wykonaj następujące kroki:

1. Pobierz odpowiedni dla twojego komputera instalator dystrybucji Kali Live USB https://www.kali.org/docs/introduction/download-official-kali-linux-images/

2. Musisz mieć pustego pen-drive'a, USB 3.0 (na USB 2.0 Kali i inne dystrybucje Linuxa mogą działać bardzo wolno ze względu na dużo wolniejszy przesył danych). Najlepiej, żeby miał min. 16GB wolnego miejsca i nie zawierał prywatnych danych, gdyż poniższa komenda zakłada ich usunięcie (nadpisanie)

3. Następnie, w celu stworzenia bootowalnego pen-drive'a podłączamy go do naszego komputera i wykonujemy następujące komendy:

```
sudo fdisk -l

# tworzymy bootowalny pen-drive z Kali Linux LIVE USB z pliku instalacyjnego
dd if=kali-linux-2020.4-live-amd64.iso of=/dev/sdb bs=4M status=progress
dd if=["ścieżka do obrazu iso"] of=["ścieżka do pen-drive"] bs=4M
status=progress
```

   Twój plik instalacyjny może mieć inną nazwę, a pen-drive może mieć inną ścieżkę dostępu, niż ww. /dev/sdb

4. Uruchamiamy komputer i w BIOS przełączamy na boot z USB Wchodzimy do BIOS, zmieniamy boot order i zapisujemy ustawienia

5. Bootujemy nasz komputer ze stworzonego Kali Linux Live USB
