Raport z Testów Penetracyjnych TryHackME "Bruteit"

Michał Lissowski

Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	0.7.11.2022
Testowana aplikacja/system	Apache httpd 2.4.29 , Linux Ubuntu

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na https://tryhackme.com/room/bruteit .

Skanowanie : nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-15 17:11 GMT
Nmap scan report for ip-10-10-188-116.eu-west-1.compute.internal (10.10.188.116)
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:0e:bf:14:fa:54:b3:5c:44:15:ed:b2:5d:a0:ac:8f (RSA)
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
|_  256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /admin/: Possible admin folder
|_  /admin/index.php: Possible admin folder
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:38:EE:49:28:69 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Opis skanowania i rekonesans

Skanowanie nmapem pokazało 2 otwarte porty. Port 22 (ssh) w wersji OpenSSH 7.6p1 oraz port 80(http) na którym działa Apache httpd 2.4.29, System operacyjny Ubuntu Linux. Za pomocą skryptu "script=default,vuln" , udalo się znaleźć ukryte foldery "/admin/: Possible admin folder , /admin/index.php: Possible admin folder. Po wejsciu na /admin pojawia się okno logowania. W kodzie znajduje się niebezpieczna informacja "!-- Hey john, if you do not remember, the username is admin". Za pomocą hydry udało się złamać hasło:
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.104.110 http-post-form "/admin/index.php:user=^USER^&pass=^PASS^&Login=Login:Username or password invalid" -V
Password=xavier. Po zalogowaniu można było pobrać RSA private key.
Narzędzie ssh2john udało się przekształcić w hash za pomocą którego można zalogować się do systemu przez ssh na konto john.

Eskalacja uprawnień i dostęp

System operacyjny Linux ubuntu. Komenda "id" dała wynik :
"uid=1001(john) gid=1001(john) groups=1001 (john),27(sudo).
Za pomcy komendy "sudo –l" znaleziono lukę : (root) NOPASSWD: /bin/cat. Oznacza to ze można używać polecenia "sudo cat" przez tego użytkownika.
Za pomocą tej podatności można odczytać zawartość /etc/shadow z hashami haseł . Narzędzie "Hashcat" ujawniło hasło roota: football.

Poniższe przedstawiona została tabela z wykrytymi podatnościami

Zagrożenie	Podatność	Opis
Krytyczne	Możliwość użycia polecenia "(root) NOPASSWD: /bin/cat" Przez zwykłego użytkownika "john"	Polecenie pozwala odczytać pliki z uprawnieniami "root". Może być użyte do ujawnienia hashy haseł co prowadzi do uzyskania dostepu do konta "root"
Wysokie	Znaczne ujawnienie informacji prowadzących do włamania.	W kodzie strony""!-- Hey john, if you do not remember, the username is admin". Rsa private key po zalogowaniu na konto "admin". Słabe hasło, łatwe do złamania np. BruteForce
Średnia	Widoczny strona logowania do administratora /admin na porcie 80	Za pomocą script=default,vuln udalo się znaleźć /admin/: Possible admin folder /admin/index.php: Possible admin folder

Podsumowanie

Zostały znalezione podatności/luki pozwalające między innymi na:

- Odczytanie informacji o użytkowniku
- Przejęcie kontroli nad dowolnym kontem użytkownika
- Łatwe złamanie hasła
- Przejęcie kontroli nad servwerem

Zalecana naprawa oraz zapobieganie

Zaleca się zmiane haseł na bardziej skomplikowane zawierające litery cyfry i znki specjalne.

Zabezpieczenie kluczy i użytkowników przed odczytem osób trzecich.

Aktualizacja systemu Linux oraz konfiguracja uprawnień użytkowników.