LABORATORIUM BEZPIECZEŃSTWO TECHNOLOGII INFORMATYCZNYCH

Data wykonania ćwiczenia:	17.10.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	3

Temat: Testowanie Odporności Systemu na Ataki Typu Brute-Force

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Cel zadania:

Celem tego laboratorium jest zapoznanie studentów z konceptem ataków typu brute-force oraz zdobycie umiejętności testowania odporności systemu na tego rodzaju ataki. Studenci będą próbować dostarczyć dowody na to, że system jest odporny na próby złamania haseł za pomocą siłowni bądź skryptów brute-force.

Część 1: Przygotowanie środowiska testowego

Najpierw wybraliśmy system operacyjny do testowania, a naszym wyborem był Kali Linux. Następnie zainstalowaliśmy Oracle VirtualBox na naszych komputerach, jeśli nie była ona już dostępna. Po tym kroku przystąpiliśmy do tworzenia nowej maszyny wirtualnej w VirtualBox. Nazwaliśmy ją "Kali Linux" i wybraliśmy odpowiednie opcje, takie jak ilość przydzielanej RAM oraz rozmiar dysku, który wynosił co najmniej 20 GB.

Następnie dostosowaliśmy naszą maszynę wirtualną, przypisując odpowiednią liczbę rdzeni CPU i podłączając obraz ISO Kali Linux jako wirtualny napęd optyczny. Po dokonaniu tych ustawień, uruchomiliśmy maszynę wirtualną i przystąpiliśmy do procesu instalacji Kali Linux.

W trakcie instalacji zostaliśmy poproszeni o wybór lokalizacji, hasła roota oraz użytkownika. Postępując zgodnie z instrukcjami na ekranie, zakończyliśmy proces instalacji. Na zakończenie tego etapu, dostosowaliśmy konfigurację systemu oraz zainstalowaliśmy dodatkowe narzędzia, aby dostosować środowisko pracy do naszych potrzeb.

Następnie musieliśmy zainstalować potrzebne nam biblioteki oraz skonfigurować ustawienia linuxa

```
┌──(igor㉿igor)-[~]
└─$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openssh-client openssh-sftp-server
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw
The following packages will be upgraded:
  openssh-client openssh-server openssh-sftp-server
3 upgraded, 0 newly installed, 0 to remove and 854 not upgraded.
Need to get 1511 kB of archives.
After this operation, 98.3 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.koyanet.lv/kali kali-rolling/main amd64 openssh-sftp-server
amd64 1:9.4p1-1 [66.3 kB]
Get:2 http://kali.koyanet.lv/kali kali-rolling/main amd64 openssh-server amd64
1:9.4p1-1 [458 kB]
Get:3 http://kali.koyanet.lv/kali kali-rolling/main amd64 openssh-client amd64
1:9.4p1-1 [986 kB]
Fetched 1511 kB in 2s (870 kB/s)
Preconfiguring packages ...
(Reading database ... 398459 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-sftp-server (1:9.4p1-1) over (1:9.3p2-1) ...
```

```
Preparing to unpack .../openssh-server_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-server (1:9.4p1-1) over (1:9.3p2-1) ...
Preparing to unpack .../openssh-client_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-client (1:9.4p1-1) over (1:9.3p2-1) ...
Setting up openssh-client (1:9.4p1-1) ...
Installing new version of config file /etc/ssh/ssh_config ...
Setting up openssh-sftp-server (1:9.4p1-1) ...
Setting up openssh-server (1:9.4p1-1) ...
Installing new version of config file /etc/ssh/moduli ...
rescue-ssh.target is a disabled or a static unit not running, not starting it.
ssh.service is a disabled or a static unit not running, not starting it.
ssh.socket is a disabled or a static unit not running, not starting it.
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for man-db (2.11.2-3) ...

┌──(igor㉿igor)-[~]
└─$ sudo nano /etc/ssh/sshd_config

┌──(igor㉿igor)-[~]
└─$ sudo service ssh restart
```

Część 2: Przeprowadzanie ataku brute-force

Aby przeprowadzić atak brute-force potrzebowaliśmy odpowiedniego narzędzia, na potrzeby zadania zainstalowaliśmy narzędzie `hydra`

```
┌──(igor㉿igor)-[~]
└─$ sudo apt-get install hydra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1).
hydra set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 854 not upgraded.
```

Następnie przygotowaliśmy plik wzięty z internetu, 500 najczęstszych haseł pośród którego było hasło naszego użytkownika.

Zdecydowałem, że atak przeprowadzimy poprzez SSH dlatego musieliśmy w tym momecie wpisać polecenie zamieniając frazy w <> na ich odpowiedniki w naszym systemie

`SSH: hydra -l <login> -P <słownik_z_hasłami> ssh://<adres_IP>:<port>`

za login ustawiliśmy nasz login czyli: `igor`

za słownik ustawiliśmy ścieżkę do naszego pliku czyli: `/home/igor/Desktop/passwords`

za adres ip wybraliśmy adres lokalny wraz z wcześniej ustawionym portem: `127.0.0.1:2222`

```

```

```
┌──(igor㉿igor)-[~]
└─$ hydra -l igor -P /home/igor/Desktop/passwords ssh://127.0.0.1:2222
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-22 16:59:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 500 login tries (l:1/p:500),
~32 tries per task
[DATA] attacking ssh://127.0.0.1:2222/
[STATUS] 97.00 tries/min, 97 tries in 00:01h, 406 to do in 00:05h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 227 to do in 00:03h, 13 active
[2222][ssh] host: 127.0.0.1   login: igor   password: 123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete
until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-22 17:05:14
```

Część 3: Monitorowanie i analiza wyników

Podczas analizy czasu potrzebnego do złamania hasła, przeprowadziliśmy atak brute-force przy użyciu narzędzia Hydra. Wynik ataku pokazał, że hasło zostało złamane, a poprawne hasło to "123". Warto zauważyć, że w trakcie ataku Hydra ostrzegał, że wiele konfiguracji SSH ogranicza liczbę równoczesnych zadań. Ostateczny wynik ataku sugeruje, że zajęło to około 6 minut (od 16:59 do 17:05).

Wygląda na to że system niestety nie podjął żadnych środków obronnych i jest to spowodowane tym że system nie zostaw skonfigurowany w odpowiedni sposób i nie miał wskazanych żadnych działań przeciwko takim attakom. Powinniśmy wcześniej zainstalować program antywirusowy, oraz systemowo wyłączyć możliwość brute-forcowania haseł, a już na samym początku powiniśmy nie ustawiać hasła, które należy do jednego z najczęściej wybieranych.

Część 4: Raport i wnioski

Podczas tego laboratorium, wykorzystując system Kali Linux na maszynie wirtualnej, przeprowadziliśmy test odporności systemu na atak typu brute-force. W ramach eksperymentu, udało nam się złamać hasło użytkownika "igor" w ciągu około 6 minut, wykorzystując narzędzie Hydra. Nasza analiza wykazała, że brak skonfigurowanych zabezpieczeń systemowych, takich jak blokowanie konta po nieudanych próbach logowania, przyczynił się do sukcesu ataku. W celu zwiększenia odporności systemu na tego rodzaju ataki, zalecamy zastosowanie środków obronnych, takich jak ustawienie trudnych haseł, monitorowanie logów systemowych, blokowanie konta po wielu próbach logowania oraz stosowanie oprogramowania antywirusowego. Warto również systematycznie aktualizować system, aby utrzymać go w bezpieczeństwie.