

Projektowanie Systemów Bezpieczeństwa

Funkcjonalność pakietu Ncrack

Spis treści

| | | |
|-----|--|----|
| 1. | Wstęp teoretyczny | 3 |
| 1.1 | Sposób działania..... | 3 |
| 1.2 | Zagrożenia związane z użyciem Ncrack | 3 |
| 2. | Przygotowanie środowiska testowego..... | 4 |
| 3. | Uzyskanie informacji na temat używanych portów za pomocą Nmap..... | 8 |
| 4. | Utworzenie plików z listą użytkowników i haseł..... | 9 |
| 5. | Testy programu ncrack dla FTP | 11 |
| 6. | Testy programu ncrack dla SSH | 14 |
| 7. | Podsumowanie..... | 17 |

1. Wstęp teoretyczny

Ncrack to narzędzie do testowania siły haseł (password cracking), które jest używane do bezpiecznego i etycznego testowania infrastruktury informatycznej pod kątem odporności na ataki oparte na próbie złamania haseł. Jest to narzędzie dostępne w otwartym źródle, zaprojektowane do przeprowadzania testów penetracyjnych oraz audytów bezpieczeństwa. Zostało stworzone w 2009 roku przez Ryana Permena w ramach projektu Google Summer of Code. Ncrack jest oprogramowaniem open-source i jest dostępne do pobrania na stronie internetowej Nmap.

1.1 Sposób działania

Ncrack działa głównie poprzez przeprowadzanie ataków typu brute-force, które polegają na próbie wielokrotnego odgadnięcia hasła poprzez przetestowanie różnych kombinacji znaków, liter, cyfr i symboli. Narzędzie obsługuje szeroki zakres protokołów sieciowych, w tym SSH, Telnet, FTP, HTTP, POP3, IMAP, SMB i RDP. Ncrack może również wykorzystywać słowniki haseł lub generować zestawy próbne w oparciu o określone wzorce.

- a) Wybór protokołu: Ncrack obsługuje różne protokoły, takie jak SSH, FTP, Telnet, HTTP, SMB itp. W zależności od tego, który protokół chcemy przetestować, ncrack jest konfigurowany w odpowiedni sposób.
- b) Określenie celu: Użytkownik określa cel ataku, czyli system, serwer lub aplikację, którą chce przetestować pod kątem siły haseł. Podawane są także dane niezbędne do nawiązania połączenia, takie jak adres IP, port, użytkownik itp.
- c) Konfiguracja parametrów: Ncrack umożliwia dostosowanie wielu parametrów ataku, takich jak rodzaj ataku (brute-force, słownikowy), prędkość ataku, czas oczekiwania między próbami itp.
- d) Uruchomienie ataku: Po skonfigurowaniu narzędzia, użytkownik uruchamia atak, który polega na automatycznym próbowaniu różnych kombinacji haseł, aż do momentu odgadnięcia prawidłowego.
- e) Analiza wyników: Po zakończeniu ataku, ncrack dostarcza raport z wynikami, informując o udanych próbach złamania hasła. W raporcie można znaleźć informacje o znalezionych hasłach, czasie trwania ataku, prędkości ataku i innych istotnych danych.

1.2 Zagrożenia związane z użyciem Ncrack

- a) Naruszenie prywatności: Nielegalne użycie Ncrack do ataków haseł na systemy, do których użytkownik nie ma uprawnień, jest naruszeniem prywatności i prawa. Może to prowadzić do poważnych konsekwencji prawnych.
- b) Nieautoryzowany dostęp: Użycie Ncrack do złamania haseł w celu uzyskania nieautoryzowanego dostępu do systemów, kont użytkowników czy danych, stanowi naruszenie zasad etyki hackingu i bezpieczeństwa informatycznego.
- c) Zablokowanie konta: Intensywne ataki siły haseł mogą prowadzić do zablokowania kont użytkowników, co może wpłynąć na dostępność usług i spowodować niedogodności dla użytkowników oraz administratorów systemów.

- d) Znaczące obciążenie sieci: Przeprowadzanie ataków siły haseł może generować znaczny ruch sieciowy i obciążenie zasobów systemowych. W przypadku intensywnych ataków, może to prowadzić do spadku wydajności systemu oraz utraty dostępności usług dla prawidłowych użytkowników.
- e) Brak zabezpieczeń i monitoringu: Ncrack i podobne narzędzia mogą być wykorzystywane przez złoczyńców do przeprowadzania ataków na słabe hasła w systemach, które nie są odpowiednio zabezpieczone ani monitorowane. To z kolei zwiększa ryzyko kompromitacji bezpieczeństwa.
- f) Społeczność i zaufanie: Użycie narzędzi do łamania haseł bez odpowiedniego uzasadnienia i uprawnień może prowadzić do utraty zaufania społeczności i klientów. Firmy i profesjonalści ds. bezpieczeństwa muszą działać zgodnie z zasadami etyki, aby utrzymać pozytywny wizerunek.

Aby zminimalizować zagrożenia związane z użyciem Ncrack, należy przestrzegać następujących zasad:

- Używać Ncrack wyłącznie do testowania bezpieczeństwa sieci.
- Nie używać Ncrack do łamania haseł do serwerów, do których nie ma się autoryzacji.
- Ustawić Ncrack tak, aby wysyłał próbne zestawy haseł z rozsądną prędkością.
- Być świadomym, że Ncrack może być wykorzystywany przez atakujących do wykrywania słabych haseł.

2. Przygotowanie środowiska testowego

Aby w sposób bezpieczny przetestować działanie programu Ncrack, wszystkie testy wykonane zostały na maszynie wirtualnej kali linux. W celu uzyskania informacji na temat otwartych portów w pierwszej kolejności za pomocą polecenia `ifconfig` wyświetliliśmy informacje o wszystkich interfejsach sieciowych aktualnie dostępnych w systemie, w tym adresy IP, adresy MAC itp

```
(root@kali)-[/home/kali/Desktop]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.19.131 netmask 255.255.255.0 broadcast 192.168.19.255
    inet6 fe80::c41:44c5:dfd:47b6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:0e:d2:7d txqueuelen 1000 (Ethernet)
    RX packets 46270 bytes 69553295 (66.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2613 bytes 159877 (156.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Za pomocą polecenia nmap (ang. „Network Mapper”), które jest narzędziem open source do eksploracji sieci i audytów bezpieczeństwa skanujemy sieć w poszukiwaniu otwartych portów i identyfikacji usług działających na tych portach wraz z informacjami o ich wersji.

Użycie: nmap [Typ(y) skanowania] [Opcje] {specyfikacja celu}

Użycie parametru -sV pozwala na wykrycie wersji usługi na otwartych portach.

```
(root@kali)-[/home/kali/Desktop]
# nmap -sV 192.168.19.131/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 08:23 EST
Nmap scan report for 192.168.19.1
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.19.2
Host is up (0.00020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  Unbound
MAC Address: 00:50:56:E2:6E:66 (VMware)

Nmap scan report for 192.168.19.254
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.19.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:8A:EA (VMware)

Nmap scan report for 192.168.19.131
Host is up (0.000010s latency).
All 1000 scanned ports on 192.168.19.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.17 seconds

(root@kali)-[/home/kali/Desktop]
#
```

W celu wykonania testów na protokole FTP, musimy najpierw skonfigurować serwer FTP. Instalujemy go za pomocą polecenia `sudo apt-get install vsftpd`

```

(root@kali)-[/home/kali/Desktop]
# sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1121 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (193 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 398680 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

```

Poleceniem `service vsftpd start` uruchamiamy serwer, a `vsftpd status` sprawdzamy czy jest on aktywny.

```

(root@kali)-[/home/kali/Desktop]
# service vsftpd start

(root@kali)-[/home/kali/Desktop]
# service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-11-28 08:27:43 EST; 14s ago
     Process: 7151 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
    Main PID: 7153 (vsftpd)
      Tasks: 1 (limit: 15395)
     Memory: 1.0M
        CPU: 15ms
    CGroup: /system.slice/vsftpd.service
            └─7153 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 28 08:27:43 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Nov 28 08:27:43 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

(root@kali)-[/home/kali/Desktop]
#

```

Za pomocą edytora nano konfigurujemy anonimowe logowanie ustawiając w pliku `vsftpd.conf` wartość `anonymous_enable` na YES.

```
GNU nano 7.2 /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on both::IPv6 and IPv4
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftp's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# Set Mark
# Copy
# To Bracket
# Where Was
# Previous
# Next
# Back
# Forward
# Prev Word
# Next Word
# Home
# End
```

Zatrzymujemy i uruchamiamy ponownie serwer FTP

```
(root@kali)-[/home/kali/Desktop]
# service vsftpd stop

(root@kali)-[/home/kali/Desktop]
# service vsftpd start

(root@kali)-[/home/kali/Desktop]
# service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-11-28 08:32:04 EST; 21s ago
   Process: 9317 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 9319 (vsftpd)
     Tasks: 1 (limit: 15395)
    Memory: 880.0K
       CPU: 13ms
    CGroup: /system.slice/vsftpd.service
            └─9319 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 28 08:32:04 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Nov 28 08:32:04 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

(root@kali)-[/home/kali/Desktop]
#
```

Możemy zalogować się teraz na FTP za pomocą anonymous/anonymous

```
(root@kali)-[/home/kali/Desktop]
# ftp 192.168.19.131
Connected to 192.168.19.131.
220 (vsFTPd 3.0.3)
Name (192.168.19.131:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```


3. Uzyskanie informacji na temat używanych portów za pomocą Nmap

Możemy zauważyć, że po instalacji serwera FTP skan za pomocą nmap wykrył nowy serwis FTP na porcie 21, który na status open. Przeprowadzimy na nim testy programu Ncrack.

```
(root@kali)-[/home/kali/Desktop]
# nmap -sV 192.168.19.131/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 08:36 EST
Nmap scan report for 192.168.19.1
Host is up (0.014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.19.2
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  Unbound
MAC Address: 00:50:56:E2:6E:66 (VMware)

Nmap scan report for 192.168.19.254
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.19.254 are in ignored states. "the quieter you be
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:8A:EA (VMware)

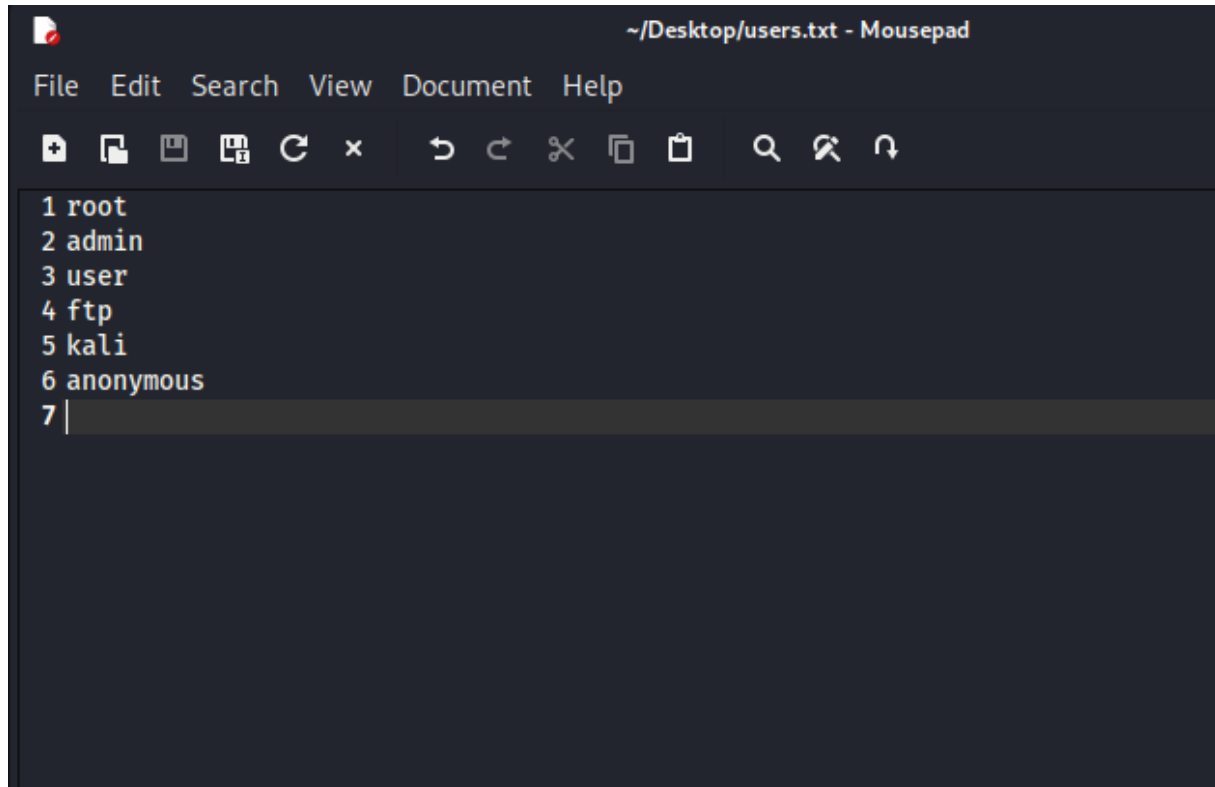
Nmap scan report for 192.168.19.131
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.39 seconds

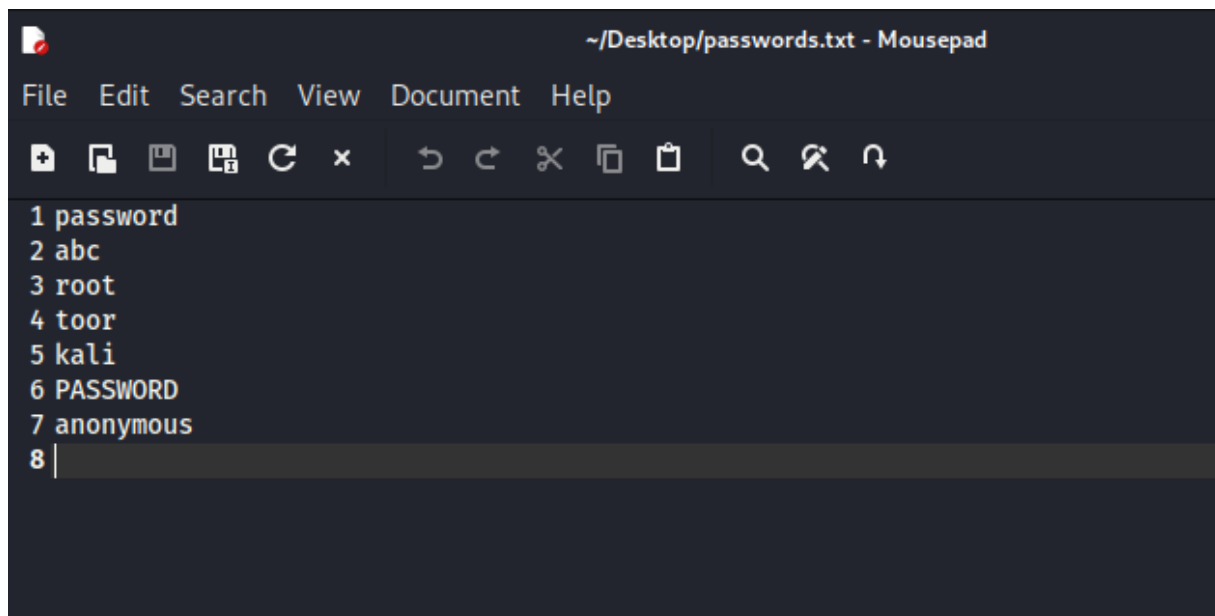
(root@kali)-[/home/kali/Desktop]
#
```


4. Utworzenie plików z listą użytkowników i haseł

Tworzymy listę użytkowników i haseł w plikach tekstowych i uzupełniamy je często używanymi nazwami użytkowników (users.txt) oraz haseł (passwords.txt).



```
~/Desktop/users.txt - Mousepad
File Edit Search View Document Help
1 root
2 admin
3 user
4 ftp
5 kali
6 anonymous
7 |
```



```
~/Desktop/passwords.txt - Mousepad
File Edit Search View Document Help
1 password
2 abc
3 root
4 toor
5 kali
6 PASSWORD
7 anonymous
8 |
```

Przykład generowania pliku tekstowego zawierającego wszystkie możliwe 4 literowe słowa:

The screenshot displays two windows from a Kali Linux desktop environment.

The top window is a terminal titled "kali@kali: ~/Desktop". It shows the following commands and output:
- Command: `(kali@kali)-[~/Desktop]
$ crunch 4 4 -o 4_letter_words.txt -t 0000`
- Output: `Crunch will now generate the following amount of data: 2284880 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 456976
crunch: 100% completed generating output`

The bottom window is a text editor titled "`~/Desktop/4_letter_words.txt` - Mousepad". Its menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for file operations like save, print, copy, paste, and search. The main text area lists 23 four-letter words generated by the tool, each preceded by a line number:

- 1 aaaA
- 2 aaab
- 3 aaac
- 4 aaad
- 5 aaae
- 6 aaaf
- 7 aaag
- 8 aaah
- 9 aaai
- 10 aaaj
- 11 aaak
- 12 aaal
- 13 aaam
- 14 aan
- 15 aaao
- 16 aaap
- 17 aaaq
- 18 aaar
- 19 aaas
- 20 aaat
- 21 aaau
- 22 aaav
- 23 aaaw

5. Testy programu ncrack dla FTP

Składnia polecenia: `ncrack [Options] {target and service specification}`

Adresem docelowym jest serwer FTP o adresie IP 192.168.19.131

Parametr `-U users.txt` oznacza, że dla nazw użytkownika użyty zostanie plik `users.txt`

Parametr `-P passwords.txt` oznacza, że dla haseł użyty zostanie plik `passwords.txt`

Po uruchomieniu polecenia `ncrack` znalazł dane uwierzytelniające. Możemy w nich zauważyć ustawione wcześniej dla serwera `anonymous`.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -U users.txt -P passwords.txt ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 08:41 EST

Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'ftp' 'password'
192.168.19.131 21/tcp ftp: 'anonymous' 'abc'
192.168.19.131 21/tcp ftp: 'anonymous' 'password'
192.168.19.131 21/tcp ftp: 'ftp' 'abc'
192.168.19.131 21/tcp ftp: 'ftp' 'toor'
192.168.19.131 21/tcp ftp: 'ftp' 'root'
192.168.19.131 21/tcp ftp: 'ftp' 'kali'
192.168.19.131 21/tcp ftp: 'ftp' 'PASSWORD'
192.168.19.131 21/tcp ftp: 'ftp' 'anonymous'

Ncrack done: 1 service scanned in 12.01 seconds.

Ncrack finished.

(root@kali)-[/home/kali/Desktop]
#
```

Przetestowanie zalogowania się na serwer FTP za pomocą znalezionej pary nazwy i hasła.
Logowanie przebiegło pomyślnie.

```
(root@kali)-[/home/kali/Desktop]
# ftp 192.168.19.131
Connected to 192.168.19.131.
220 (vsFTPd 3.0.3)
Name (192.168.19.131:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Możemy również zmienić sposób iteracji listy za pomocą parametru `--passwords-first`. Przeszukana zostanie lista haseł dla każdej nazwy użytkownika, gdzie domyślnie sytuacja jest odwrotna.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -U users.txt -P passwords.txt --passwords-first ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 09:19 EST

Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'ftp' 'abc'
192.168.19.131 21/tcp ftp: 'ftp' 'root'
192.168.19.131 21/tcp ftp: 'ftp' 'toor'
192.168.19.131 21/tcp ftp: 'ftp' 'kali'
192.168.19.131 21/tcp ftp: 'ftp' 'password'
192.168.19.131 21/tcp ftp: 'anonymous' 'password'
192.168.19.131 21/tcp ftp: 'anonymous' 'toor'
192.168.19.131 21/tcp ftp: 'anonymous' 'anonymous'

Ncrack done: 1 service scanned in 18.05 seconds.

Ncrack finished.

(root@kali)-[/home/kali/Desktop]
#
```

Parametr `--pairwise` wybiera nazwę użytkownika oraz hasło parami z plików. Jak można zauważyć na poniższym zrzucie ekranu, otrzymaliśmy dużo mniej znalezionych opcji niż w poprzednich przypadkach.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -U users.txt -P passwords.txt --pairwise ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 09:21 EST

Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'anonymous' 'PASSWORD'
192.168.19.131 21/tcp ftp: 'ftp' 'toor'
192.168.19.131 21/tcp ftp: 'kali' 'kali'

Ncrack done: 1 service scanned in 15.00 seconds.

Ncrack finished.

(root@kali)-[/home/kali/Desktop]
#
```

Parametr `--user` pozwala na użycie określonej nazwy użytkownika zamiast podawania listy nazw.

```
(root@kali)-[/home/kali/Desktop]
# ncrack --user ftp -P passwords.txt ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 09:23 EST
Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'ftp' 'password'

Ncrack done: 1 service scanned in 3.00 seconds.

Ncrack finished.
#
```

Analogicznie parametr `--pass` pozwala na użycie określonego hasła zamiast podawania listy haseł.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -U users.txt --pass password ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 09:24 EST

Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'ftp' 'password'
192.168.19.131 21/tcp ftp: 'anonymous' 'password'

Ncrack done: 1 service scanned in 12.01 seconds.

Ncrack finished.
#
```

Parametr -f zatrzymuje działanie programu po znalezieniu pierwszego wyniku. Może to być przydatne, gdy dysponujemy plikami o dużych rozmiarach.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -f -U users.txt -P passwords.txt ftp://192.168.19.131

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-28 09:26 EST
user:mysql.txt
Discovered credentials for ftp on 192.168.19.131 21/tcp:
192.168.19.131 21/tcp ftp: 'ftp' 'abc'

Ncrack done: 1 service scanned in 12.01 seconds.

Ncrack finished.
passwords
(root@kali)-[/home/kali/Desktop]
#
```

6. Testy programu ncrack dla SSH

Po instalacji OpenSSH Server w pliku sshd_config ustawiamy możliwość PasswordAuthentication na yes, co umożliwi użycie loginu i hasła.

```
(kali@kali)-[~/Desktop]
$ sudo nano /etc/ssh/sshd_config
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
```

Restartujemy serwis SSH

```
(kali@kali)-[~/Desktop]
$ sudo service ssh restart
```

Po instalacji port 22 ma status otwarty

```
Nmap scan report for 192.168.142.130
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.4p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 14.54 seconds
```

Dodanie nowych użytkowników i ustawienie im hasła.

```
(kali㉿kali)-[~/Desktop] [sudo] password for kali:
$ sudo adduser admin
info: Adding user `admin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `admin' (1002) ...
info: Adding new user `admin' (1002) with group `admin (1002)' ...
info: Creating home directory `/home/admin' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
info: Adding new user `admin' to supplemental / extra groups `users' ...
info: Adding user `admin' to group `users' ...
```



```

(kali㉿kali)-[~/Desktop]
$ ssh admin@192.168.142.130
The authenticity of host '192.168.142.130 (192.168.142.130)' can't be established.
ED25519 key fingerprint is SHA256:VXyfT+vjEyG8SFMJmwvP3rIfX6HFMv+7lD+IRdw60IQ
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.142.130' (ED25519) to the list of known hosts.
admin@192.168.142.130's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(admin㉿kali)-[~]
$ █

```

```

(kali㉿kali)-[~/Desktop]
$ sudo adduser sstest
info: Adding user `sstest' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `sstest' (1003) ...
info: Adding new user `sstest' (1003) with group `sstest (1003)' ...
info: Creating home directory `/home/sstest' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sstest
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
info: Adding new user `sstest' to supplemental / extra groups `users' ...
info: Adding user `sstest' to group `users' ...

```

Po dodaniu do listy użytkowników i haseł nazwy użytkownika sstest, program ncrack znalazł dane uwierzytniające dla obu utworzonych użytkowników.

```
(root@kali)-[/home/kali/Desktop]
# ncrack -p 22 -U users.txt -P passwords.txt 192.168.142.130

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-12-18 15:45 EST

Discovered credentials for ssh on 192.168.142.130 22/tcp:
192.168.142.130 22/tcp ssh: 'admin' 'root'
192.168.142.130 22/tcp ssh: 'sstest' 'password'

Ncrack done: 1 service scanned in 6.00 seconds.

Ncrack finished.
```

7. Podsumowanie

Ncrack jest narzędziem do testowania siły haseł, zaprojektowanym do bezpiecznego i etycznego przeprowadzania testów penetracyjnych oraz audytów bezpieczeństwa. Działa poprzez przeprowadzanie ataków typu brute-force, testując różne kombinacje haseł w celu zidentyfikowania potencjalnych słabości w systemach autentykacji. Nasze testy przeprowadzaliśmy za pomocą protokołu FTP(File Transfer Protocol) oraz SSH (Secure Shell). Ncrack może być skutecznym narzędziem do łamania haseł w serwerach FTP. Działa poprzez próby wielu kombinacji loginu i hasła, co pozwala zidentyfikować słabe punkty w konfiguracji FTP. Ncrack może być wykorzystywany do ataków na serwery SSH, jednak ze względu na silne zabezpieczenia tego protokołu, skuteczność może być ograniczona, zwłaszcza przy użyciu długich i złożonych haseł. Aby zwiększyć bezpieczeństwo serwera SSH, zaleca się korzystanie z kluczy SSH, ograniczanie dostępu tylko do niezbędnych użytkowników, stosowanie odpowiednich reguł firewalla oraz monitorowanie logów w celu szybkiego wykrywania ewentualnych ataków.