5 ways to Banner Grabbing

posted in FOOTPRINTING , PENETRATION TESTING on JULY 12, 2017 by RAJ CHANDEL

SHARE

Banner are refers as text message that received from host. Banners usually contain information about a service, such as the version number.

From Wikipedia

Banner grabbing is a process to collect details regarding any remote PC on a network and the services running on its open ports. An attacker can make use of banner grabbing in order to discover network hosts and running services with their versions on their open ports and more over operating systems so that he can exploits it.

Nmap

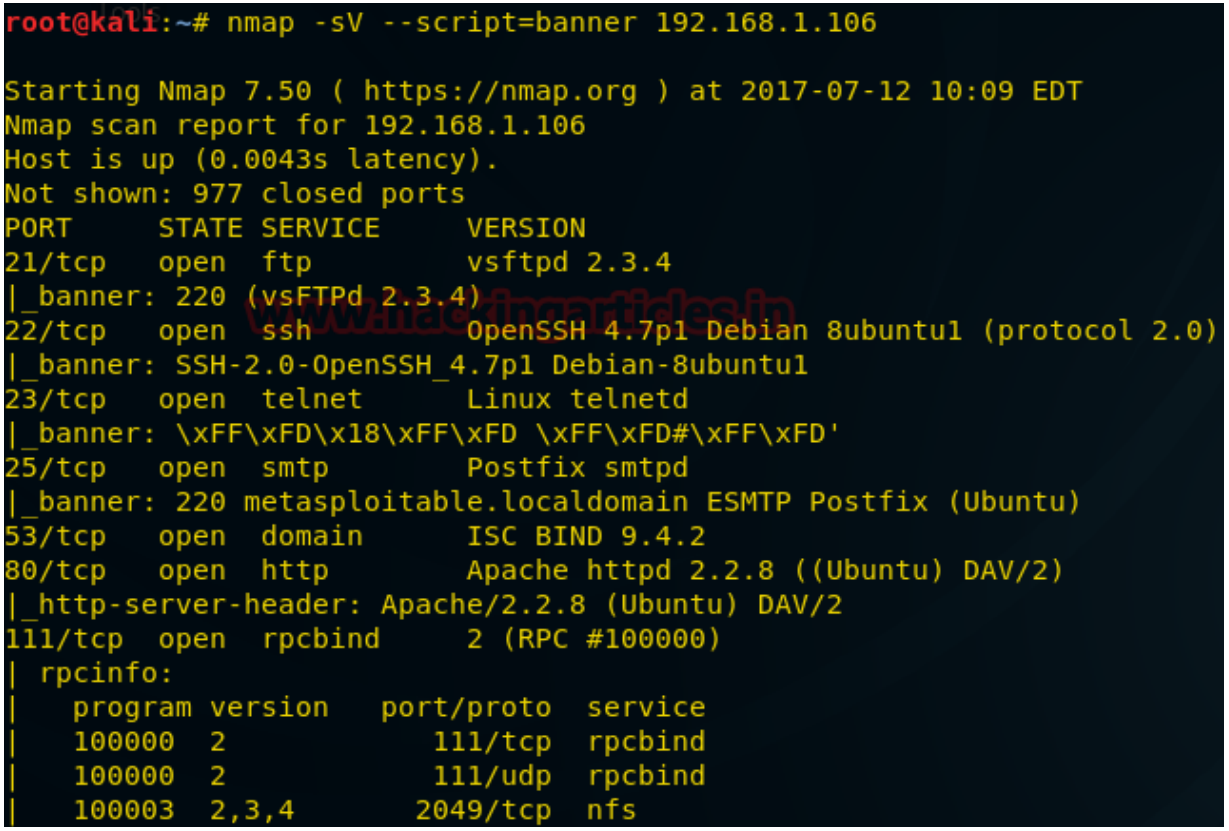
A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.

The banner will be shortened to fit into a single line, but an extra line may be printed for every increase in the level of verbosity requested on the command line.

Type following command which will fetch banner for every open port in remote PC.

```
1 nmap -sV --script=banner 192.168.1.106
```

From screenshot you can read the services and their version for open ports fetched by NMAP Script to grab banner for the target 192.168.1.106



```
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      55010/udp  mountd
|   100005  1,2,3      56414/tcp  mountd
|   100021  1,3,4      37454/udp  nlockmgr
|   100021  1,3,4      41196/tcp  nlockmgr
|   100024  1          36246/udp  status
|_  100024  1          37643/tcp  status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
|_banner: \x01Where are you?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
|_banner: root@metasploitable:/#
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.106]
```

Following command will grab the banner for selected port i.e. **80** for http service and version.

```
1 nmap -Pn -p 80 -sV --script=banner 192.168.1.106
```

As result it will dumb "http-server-header: Apache/2.2.8 (Ubuntu) DAV/2"

```
root@kali:~# nmap -Pn -p 80 -sV --script=banner 192.168.1.106

Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-12 10:16 EDT
Nmap scan report for 192.168.1.106
Host is up (0.0066s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 38:B1:DB:B3:BC:D9 (Hon Hai Precision Ind.)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.41 seconds
```

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

CURL

Curl –I is use for head in order to shown document information only; type following command to grab **HTTP banner** of remote PC.

```
curl -s -I 192.168.1.106 | grep -e "Server: "
```

As result it will dumb “http-server-header: Apache/2.2.8 (Ubuntu) DAV/2”

```
root@kali:~# curl -s -I 192.168.1.106 | grep -e "Server: "
Server: Apache/2.2.8 (Ubuntu) DAV/2
root@kali:~#
```

Telnet

Type following command to grab **SSH banner** of remote PC.

```
telnet 192.168.1.106 22
```

As result it will dumb “SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1”

```
oot@kali:~# telnet 192.168.1.106 22
rying 192.168.1.106...
onnected to 192.168.1.106.
scape character is '^]'.
SH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Netcat

Type following command to grab **SSH banner** of remote PC.

```
nc -v 192.168.1.106 22
```

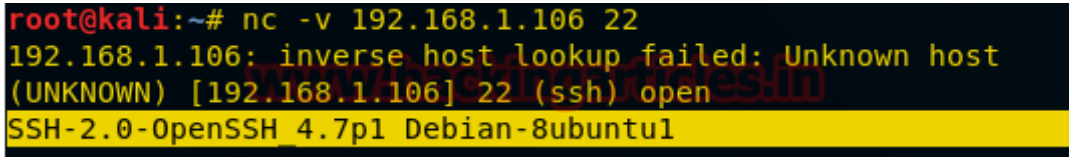
As result it will dumb “SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1”

Articles

Select Month

Facebook Page

Be the first of your friends to like this



Dmitry

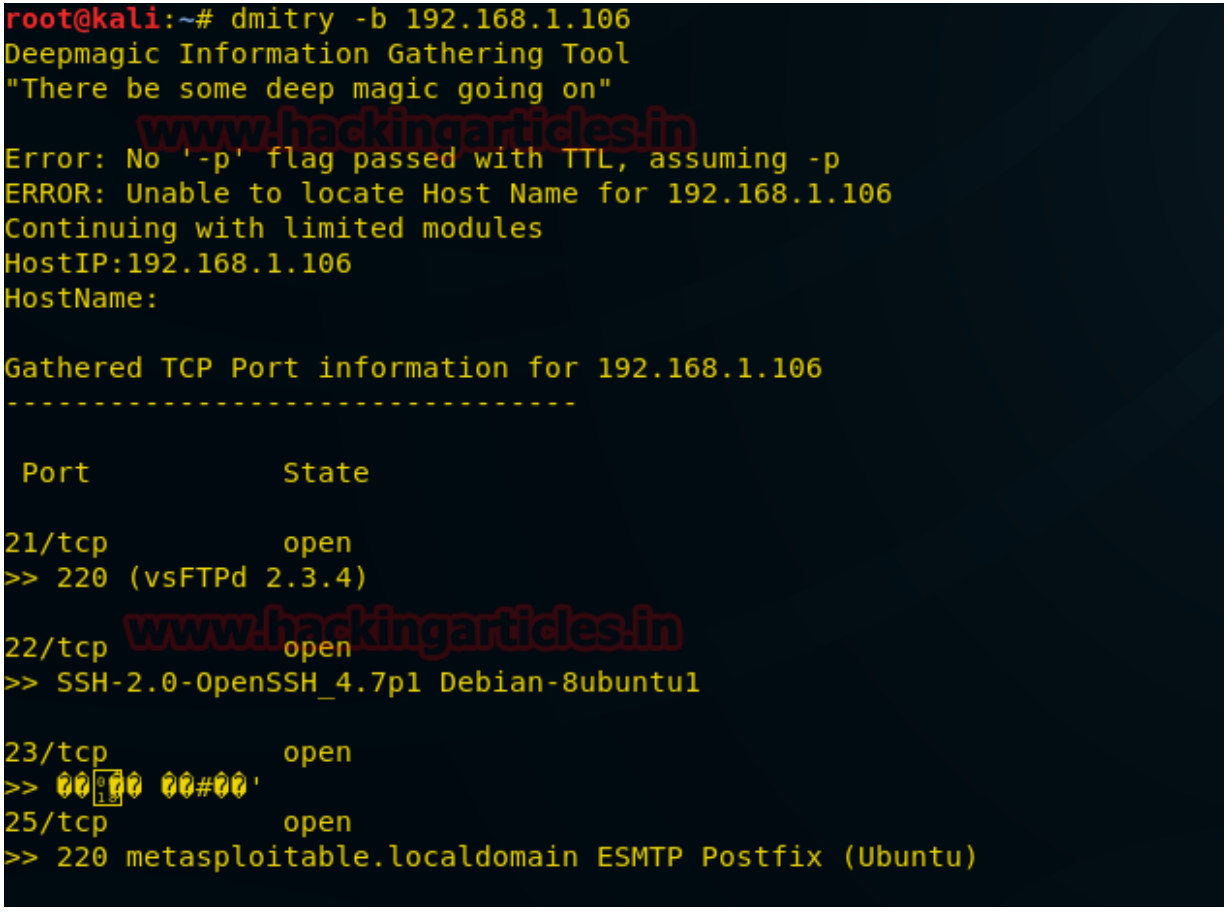
DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

Dmitry –**b** is use for banner grabbing for all open ports; Type following command to grab **SSH banner** of remote PC.

```
dmitry -b 192.168.1.106
```

From screenshot you can see it has shown banner for open port **21, 22, 23** and **25**.

In this way Attacker can grab the services and their version for open ports on remote PC



Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST
← BEGINNER GUIDE TO METERPRETER (PART 1)

NEXT POST
5 WAYS TO CRAWL A WEBSITE →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Notify me of follow-up comments by email.

Notify me of new posts by email.