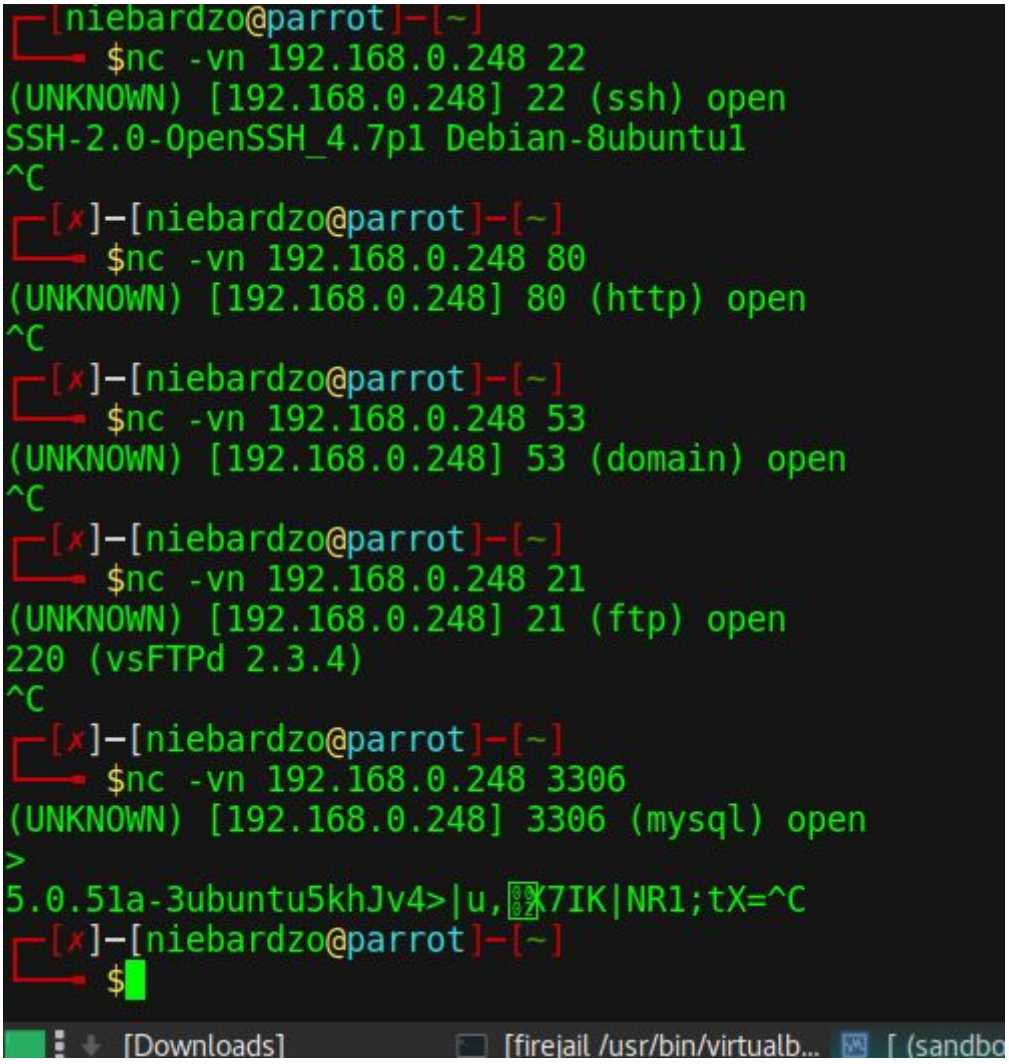
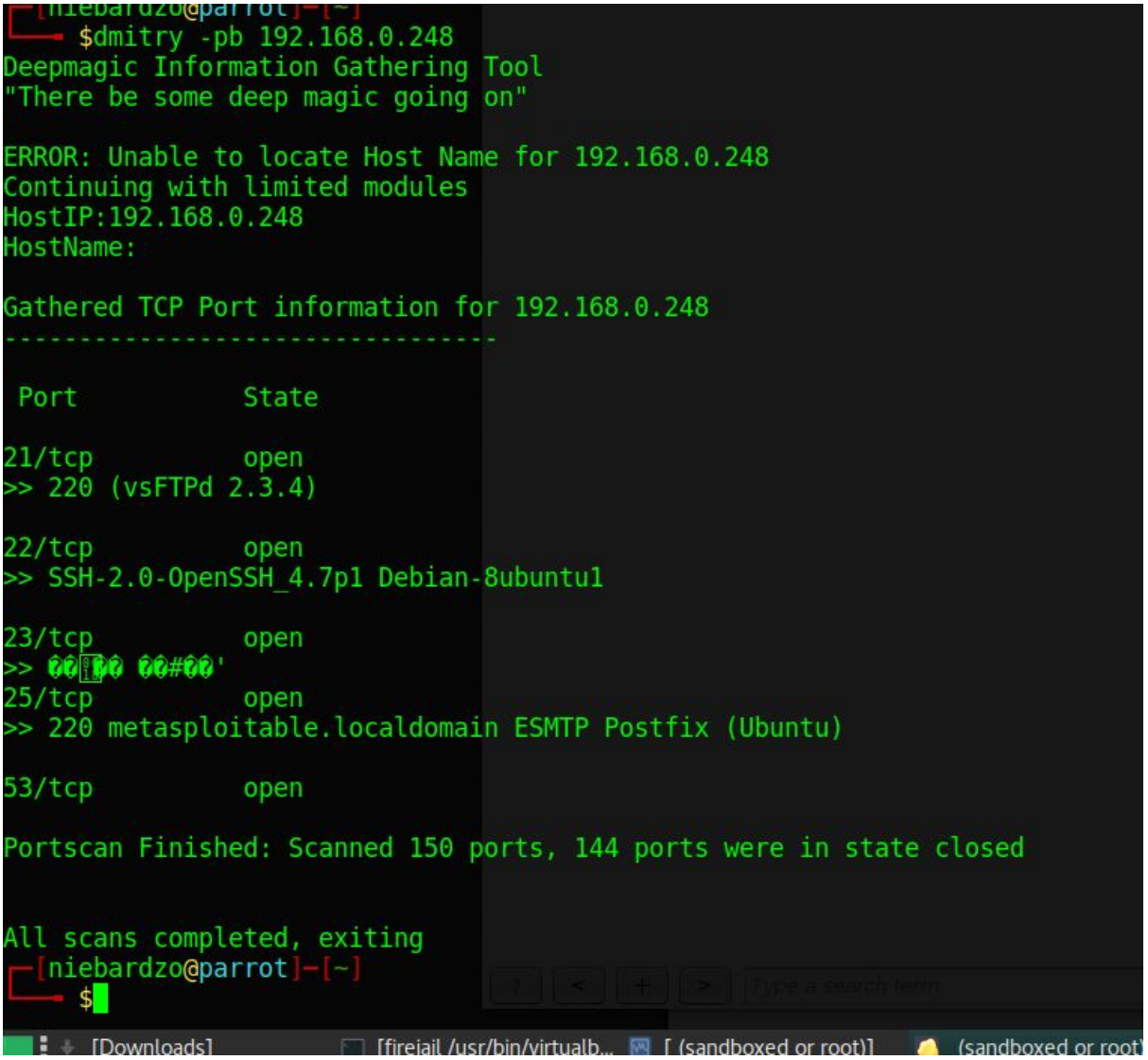
5. Identyfikacja usług sieciowych na podstawie bannerów.

Z użyciem programu netcat, wykrywanie bannerów na konkretnym porcie:



Jak widać na screenshocie niektóre usługi takie jak: SSH, FTP, MySQL zwracają informację o wersji. Można w ten sposób łatwo zidentyfikować usługę działającą na systemie. Niektóre z usług takie jak DNS lub HTTP nie udostępniają informacji w bannerach.



Z użyciem programu dmitry możemy w zautomatyzowany sposób odczytać bannery poszczególnych usług. Jak widać na screenshocie, oprócz ssh i ftp usługi które udostępniają bannery działają na portach telnet - port 23 i postfix - port 25.

```
[niebardzo@parrot]-[~]
$sudo nmap -sT 192.168.0.248 -p 1-200 --script=banner

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-09 15:20 CDT
Nmap scan report for 192.168.0.248
Host is up (0.0074s latency).
Not shown: 192 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp  open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp  open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp  open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
MAC Address: 08:00:27:3A:0F:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
[niebardzo@parrot]-[~]
$
```

Jak widać nmap zwrócił te same bannery co dmitry dla przeskanowanych portów od 1 do 200.

Następnie użyte zostanie narzędzie amap do przeskanowania portów od 1 do 2000.

```
$amap -B 192.168.0.248 1-2000
amap v5.4 (www.thc.org/thc-amap) started at 2018-05-09 15:23:50 - BANNER mode

Banner on 192.168.0.248:25/tcp : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n
Banner on 192.168.0.248:1524/tcp : root@metasploitable/#
Banner on 192.168.0.248:512/tcp : Where are you?\n
Banner on 192.168.0.248:21/tcp : 220 (vsFTPd 2.3.4)\r\n
Banner on 192.168.0.248:22/tcp : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n
Banner on 192.168.0.248:23/tcp :  #'

amap v5.4 finished at 2018-05-09 15:24:01
[niebardzo@parrot]-[~]
$
```

Dodatkowo znaleźliśmy usługi udostępniające bannery na portach: 512, 1524.

6. Identyfikacja usług które nie przedstawiają się bannerem.

```
$sudo nmap -nv 192.168.0.248 -p 80

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-09 15:33 CDT
Initiating ARP Ping Scan at 15:33
Scanning 192.168.0.248 [1 port]
Completed ARP Ping Scan at 15:33, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:33
Scanning 192.168.0.248 [1 port]
Discovered open port 80/tcp on 192.168.0.248
Completed SYN Stealth Scan at 15:33, 0.05s elapsed (1 total ports)
Nmap scan report for 192.168.0.248
Host is up (0.00034s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:3A:0F:F1 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
[niebardzo@parrot]-[~]
 $
```

Nmap nie wykrył wersji usługi która działa na porcie 80. Następne skanowanie odbędzie się z flagą -sV najpopularniejszych portów.

```
[niebardzo@parrot]-[~]
 $sudo nmap 192.168.0.248 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-09 15:38 CDT
Nmap scan report for 192.168.0.248
Host is up (0.00059s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
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
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:3A:0F:F1 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Lin

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds
[niebardzo@parrot]-[~]
 $
```

Jak widać serwer ma sporo działających usług których wersje zostały zidentyfikowane przez Nmapa.