P.T Project

By Stanislav Kolbeshkin

As a part of Cyber studying in John Bryce we were asked to make an automated process with a script to scan a range or a single ip address and map it vurnlabilities and weak credentials, the tools we were suggest to use is nmap and masscan for active scanning. Its pointless to say that the P.T world finished in this small procedure, the PT world is huge and contains a lot of other points of interest as auxilliries used by msfconsole and more.

In this project we just showed the little of the huge and amazing world of Penetration Testing!

In my project I was using nmap to scan the client with hes input of the range he would like to test, needless to say the higher the count of the addresses the more time it would take, because of the high time wait we gave the client an option, to choose between the basic scan and the full scan options, the difference between them in the depth that each scan goes, in the basic scan you would only get the visible version of service's you run, the services themselves and open UDP ports that could be use for infiltration.

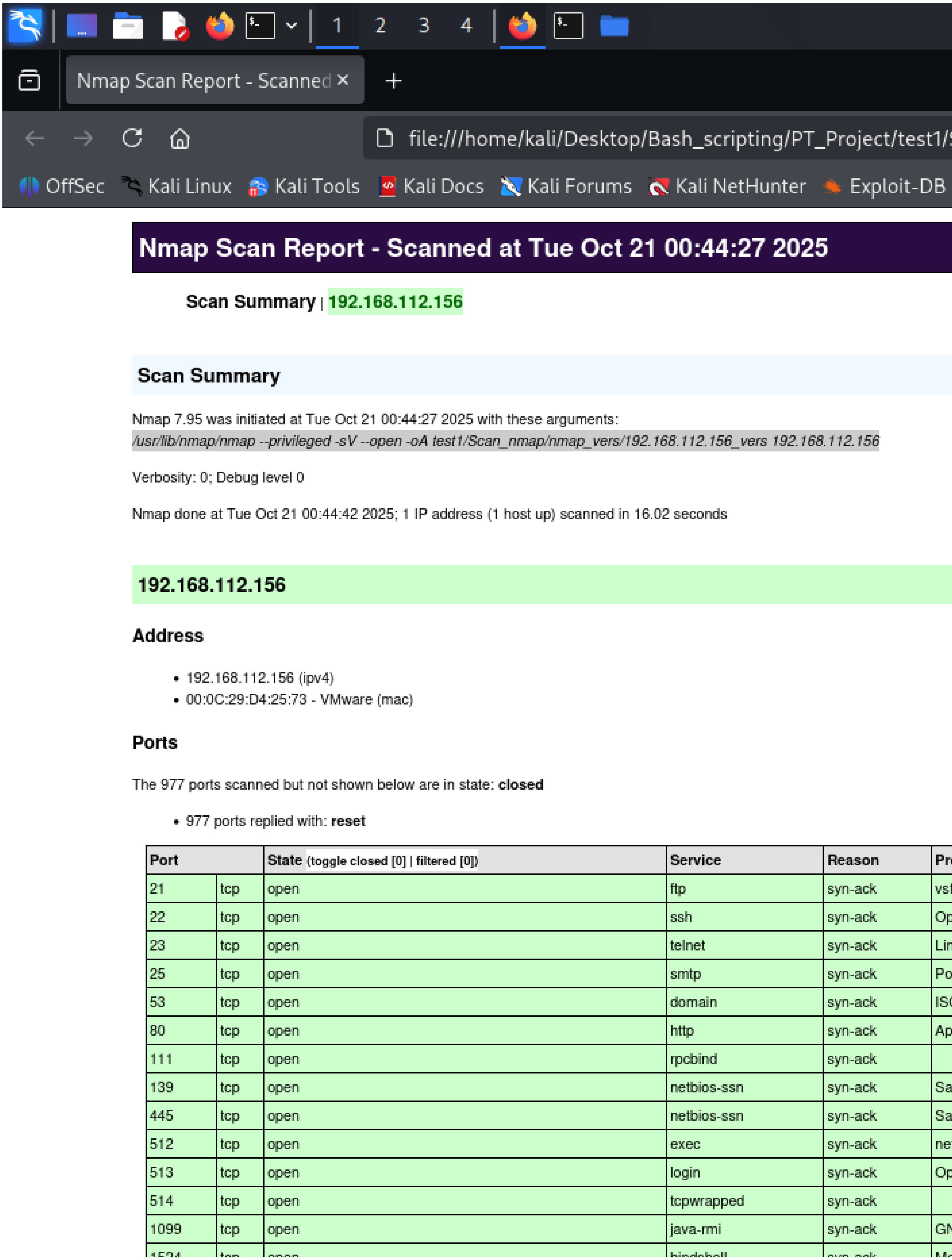
On the other hand the full scan goes even deeper testing the malwares vulnerabilities and even credentials that's can be gathered or tested by the client input.

At the end the client can check the reports with created html file for comfortable view and to zip all the results with the reports as he would like.

The project was tough, it holds an amazing potential for creativity and creation which with every new opening of its code endet up in extra hours perfecting and tunning each line into something more sophisticated.

With the help of our teacher Doron Zohar and a little bit tunning of deepseek Ai I was able to reach a finishing point of the project!

Here are some pictures from it as it ran:


1
2
3
4
Nmap Scan Report - Scanned
file:///home/kali/Desktop/Bash_scripting/PT_Project/test1/S
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB

Nmap Scan Report - Scanned at Tue Oct 21 00:44:27 2025

Scan Summary | 192.168.112.156

Scan Summary

Nmap 7.95 was initiated at Tue Oct 21 00:44:27 2025 with these arguments:

```
/usr/lib/nmap/nmap --privileged -sV --open -oA test1/Scan_nmap/nmap_vers/192.168.112.156_vers 192.168.112.156
```

Verbosity: 0; Debug level 0

Nmap done at Tue Oct 21 00:44:42 2025; 1 IP address (1 host up) scanned in 16.02 seconds

192.168.112.156

Address

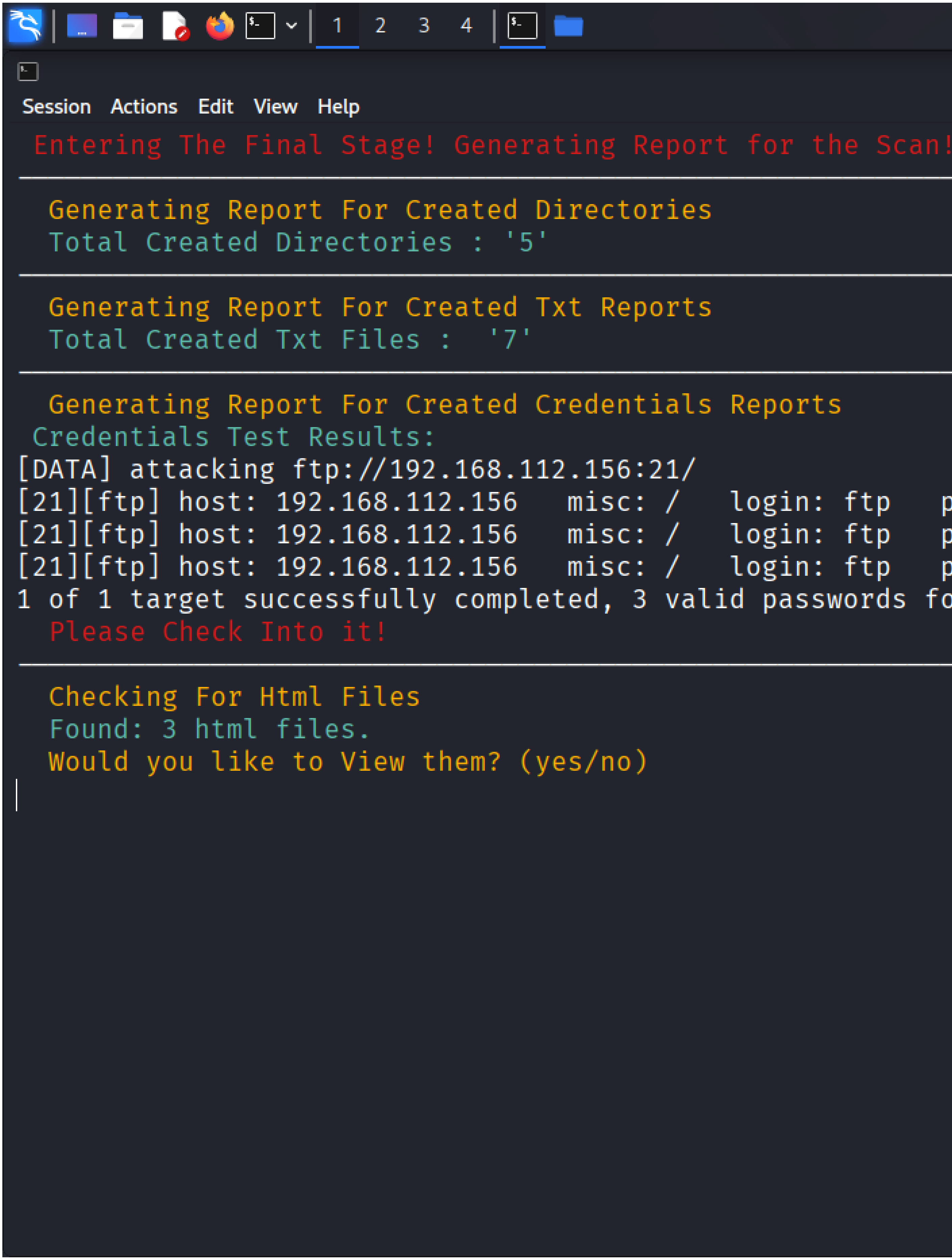
- 192.168.112.156 (ipv4)
- 00:0C:29:D4:25:73 - VMware (mac)

Ports

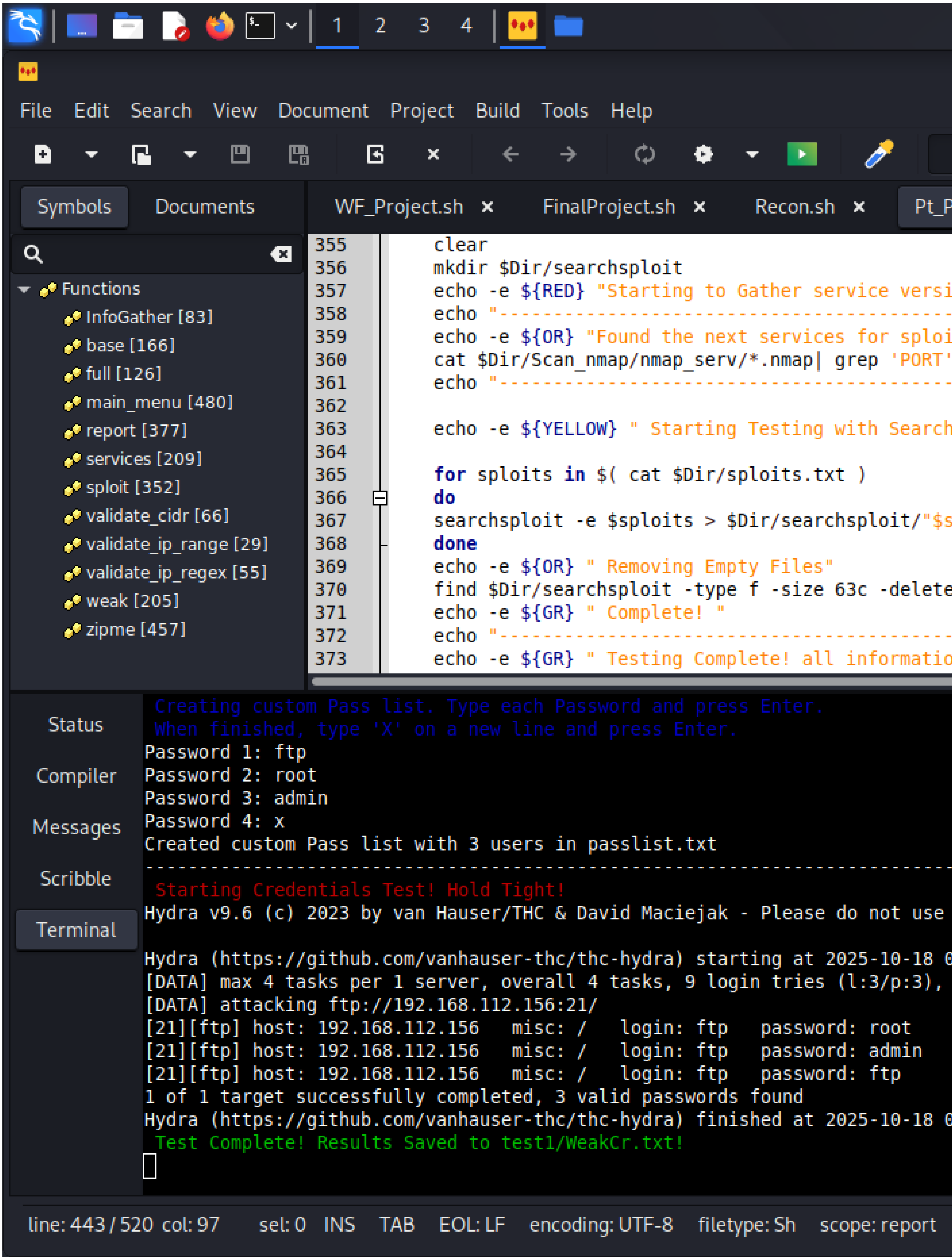
The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Pr
21	tcp	open	ftp	syn-ack	vsf
22	tcp	open	ssh	syn-ack	Op
23	tcp	open	telnet	syn-ack	Lin
25	tcp	open	smtp	syn-ack	Po
53	tcp	open	domain	syn-ack	ISC
80	tcp	open	http	syn-ack	Ap
111	tcp	open	rpcbind	syn-ack	
139	tcp	open	netbios-ssn	syn-ack	Sa
445	tcp	open	netbios-ssn	syn-ack	Sa
512	tcp	open	exec	syn-ack	ne
513	tcp	open	login	syn-ack	Op
514	tcp	open	tcpwrapped	syn-ack	
1099	tcp	open	java-rmi	syn-ack	GN
1524	tcp	open	bindshell	syn-ack	M



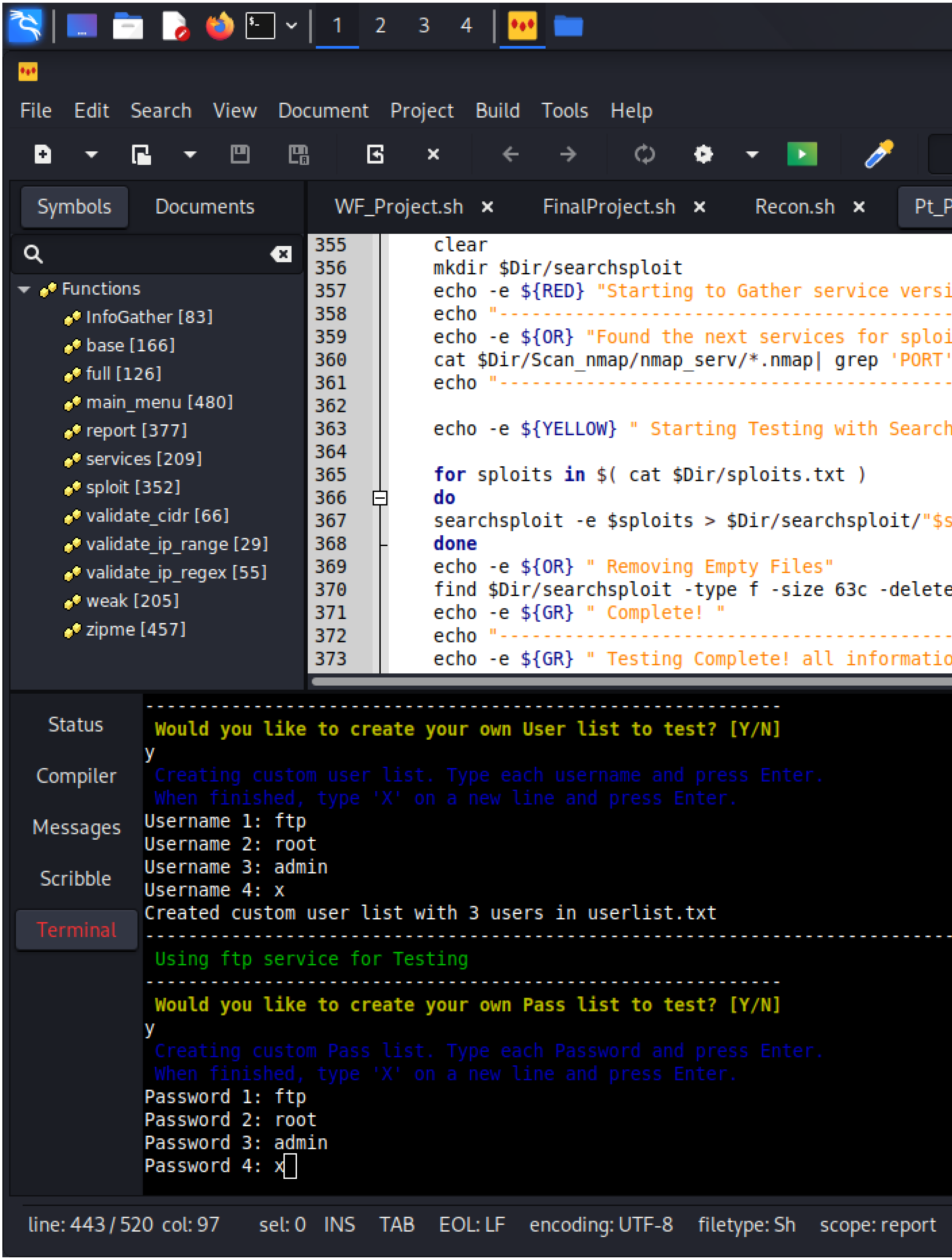
```
 Entering The Final Stage! Generating Report for the Scan!
─────────────────────────────────────────────────────────────
   Generating Report For Created Directories
   Total Created Directories : '5'
─────────────────────────────────────────────────────────────
   Generating Report For Created Txt Reports
   Total Created Txt Files :  '7'
─────────────────────────────────────────────────────────────
   Generating Report For Created Credentials Reports
  Credentials Test Results:
[DATA] attacking ftp://192.168.112.156:21/
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   p
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   p
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   p
1 of 1 target successfully completed, 3 valid passwords fo
   Please Check Into it!
─────────────────────────────────────────────────────────────
   Checking For Html Files
   Found: 3 html files.
   Would you like to View them? (yes/no)
```



```
    clear
    mkdir $Dir/searchsploit
    echo -e ${RED} "Starting to Gather service versi
    echo "-----------------------------------------
    echo -e ${OR} "Found the next services for sploi
    cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
    echo "-----------------------------------------

    echo -e ${YELLOW} " Starting Testing with Search

    for sploits in $( cat $Dir/sploits.txt )
    do
    searchsploit -e $sploits > $Dir/searchsploit/"$s
    done
    echo -e ${OR} " Removing Empty Files"
    find $Dir/searchsploit -type f -size 63c -delete
    echo -e ${GR} " Complete! "
    echo "-----------------------------------------
    echo -e ${GR} " Testing Complete! all informatio
```

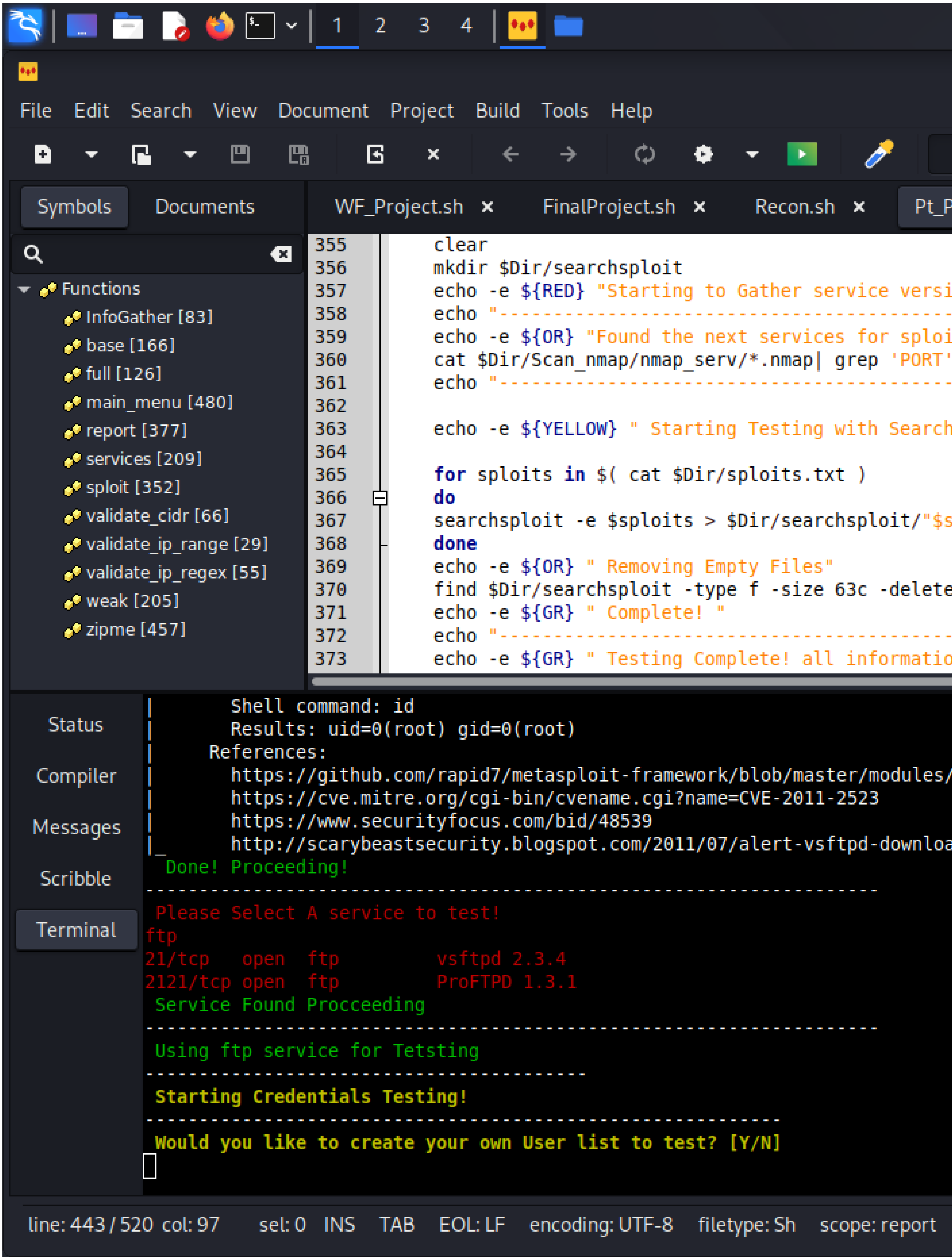
```
 Creating custom Pass list. Type each Password and press Enter.
 When finished, type 'X' on a new line and press Enter.
Password 1: ftp
Password 2: root
Password 3: admin
Password 4: x
Created custom Pass list with 3 users in passlist.txt
------------------------------------------------------------
 Starting Credentials Test! Hold Tight!
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-18 0
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3),
[DATA] attacking ftp://192.168.112.156:21/
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   password: root
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   password: admin
[21][ftp] host: 192.168.112.156   misc: /   login: ftp   password: ftp
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-18 0
 Test Complete! Results Saved to test1/WeakCr.txt!
```

line: 443 / 520 col: 97   sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: report



```
    clear
    mkdir $Dir/searchsploit
    echo -e ${RED} "Starting to Gather service versi
    echo "------------------------------------------
    echo -e ${OR} "Found the next services for sploi
    cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
    echo "------------------------------------------

    echo -e ${YELLOW} " Starting Testing with Search

    for sploits in $( cat $Dir/sploits.txt )
    do
    searchsploit -e $sploits > $Dir/searchsploit/"$s
    done
    echo -e ${OR} " Removing Empty Files"
    find $Dir/searchsploit -type f -size 63c -delete
    echo -e ${GR} " Complete! "
    echo "------------------------------------------
    echo -e ${GR} " Testing Complete! all informatio
```

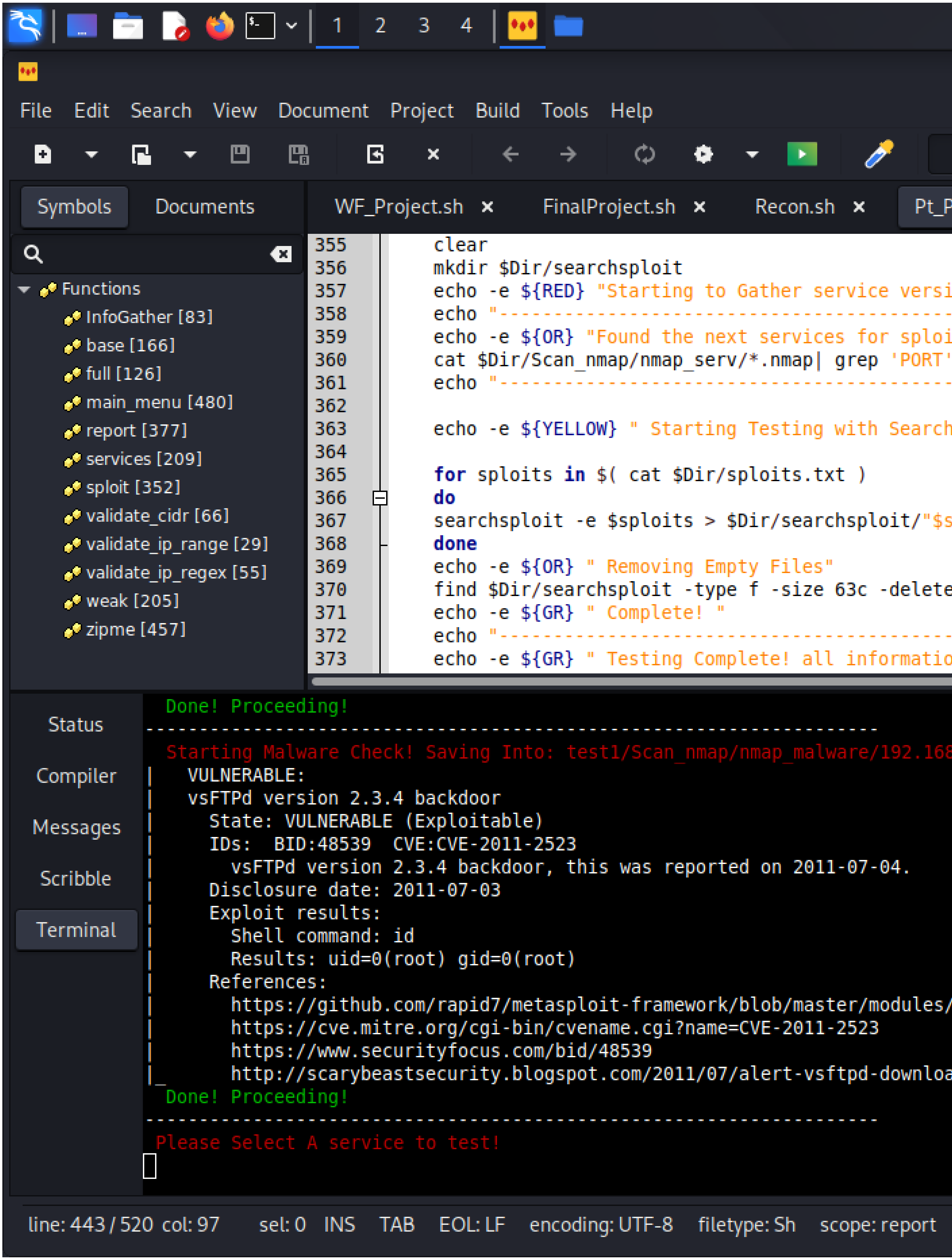
```
-------------------------------------------------------------
 Would you like to create your own User list to test? [Y/N]
y
 Creating custom user list. Type each username and press Enter.
 When finished, type 'X' on a new line and press Enter.
Username 1: ftp
Username 2: root
Username 3: admin
Username 4: x
Created custom user list with 3 users in userlist.txt
-----------------------------------------------------------------------
 Using ftp service for Testing
-------------------------------------------------------------
 Would you like to create your own Pass list to test? [Y/N]
y
 Creating custom Pass list. Type each Password and press Enter.
 When finished, type 'X' on a new line and press Enter.
Password 1: ftp
Password 2: root
Password 3: admin
Password 4: x
```



```
clear
mkdir $Dir/searchsploit
echo -e ${RED} "Starting to Gather service versi
echo "-----------------------------------------
echo -e ${OR} "Found the next services for sploi
cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
echo "-----------------------------------------

echo -e ${YELLOW} " Starting Testing with Search

for sploits in $( cat $Dir/sploits.txt )
do
searchsploit -e $sploits > $Dir/searchsploit/"$s
done
echo -e ${OR} " Removing Empty Files"
find $Dir/searchsploit -type f -size 63c -delete
echo -e ${GR} " Complete! "
echo "-----------------------------------------
echo -e ${GR} " Testing Complete! all informatio
```

```
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downloa
 Done! Proceeding!
--------------------------------------------------------------------
 Please Select A service to test!
ftp
21/tcp   open  ftp         vsftpd 2.3.4
2121/tcp open  ftp         ProFTPD 1.3.1
 Service Found Procceeding
--------------------------------------------------------------------
 Using ftp service for Tetsting
-----------------------------------------
 Starting Credentials Testing!
-----------------------------------------------------------
 Would you like to create your own User list to test? [Y/N]
```

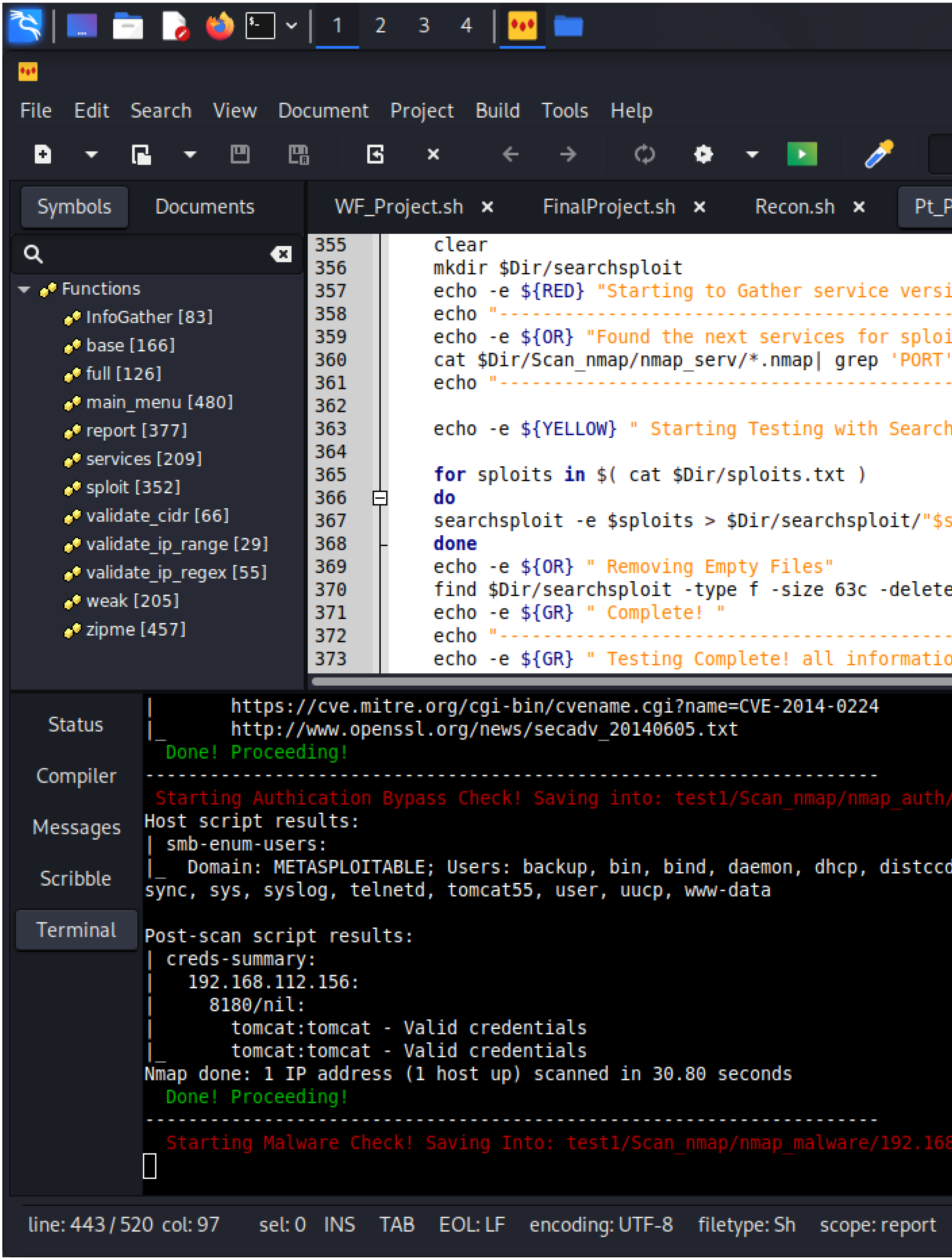
line: 443 / 520 col: 97 sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: report



```
    clear
    mkdir $Dir/searchsploit
    echo -e ${RED} "Starting to Gather service versi
    echo "------------------------------------------
    echo -e ${OR} "Found the next services for sploi
    cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
    echo "------------------------------------------

    echo -e ${YELLOW} " Starting Testing with Search

    for sploits in $( cat $Dir/sploits.txt )
    do
    searchsploit -e $sploits > $Dir/searchsploit/"$s
    done
    echo -e ${OR} " Removing Empty Files"
    find $Dir/searchsploit -type f -size 63c -delete
    echo -e ${GR} " Complete! "
    echo "------------------------------------------
    echo -e ${GR} " Testing Complete! all informatio
```

```
  Done! Proceeding!
--------------------------------------------------------------------
  Starting Malware Check! Saving Into: test1/Scan_nmap/nmap_malware/192.168
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       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://github.com/rapid7/metasploit-framework/blob/master/modules/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downloa
  Done! Proceeding!
--------------------------------------------------------------------
 Please Select A service to test!
```

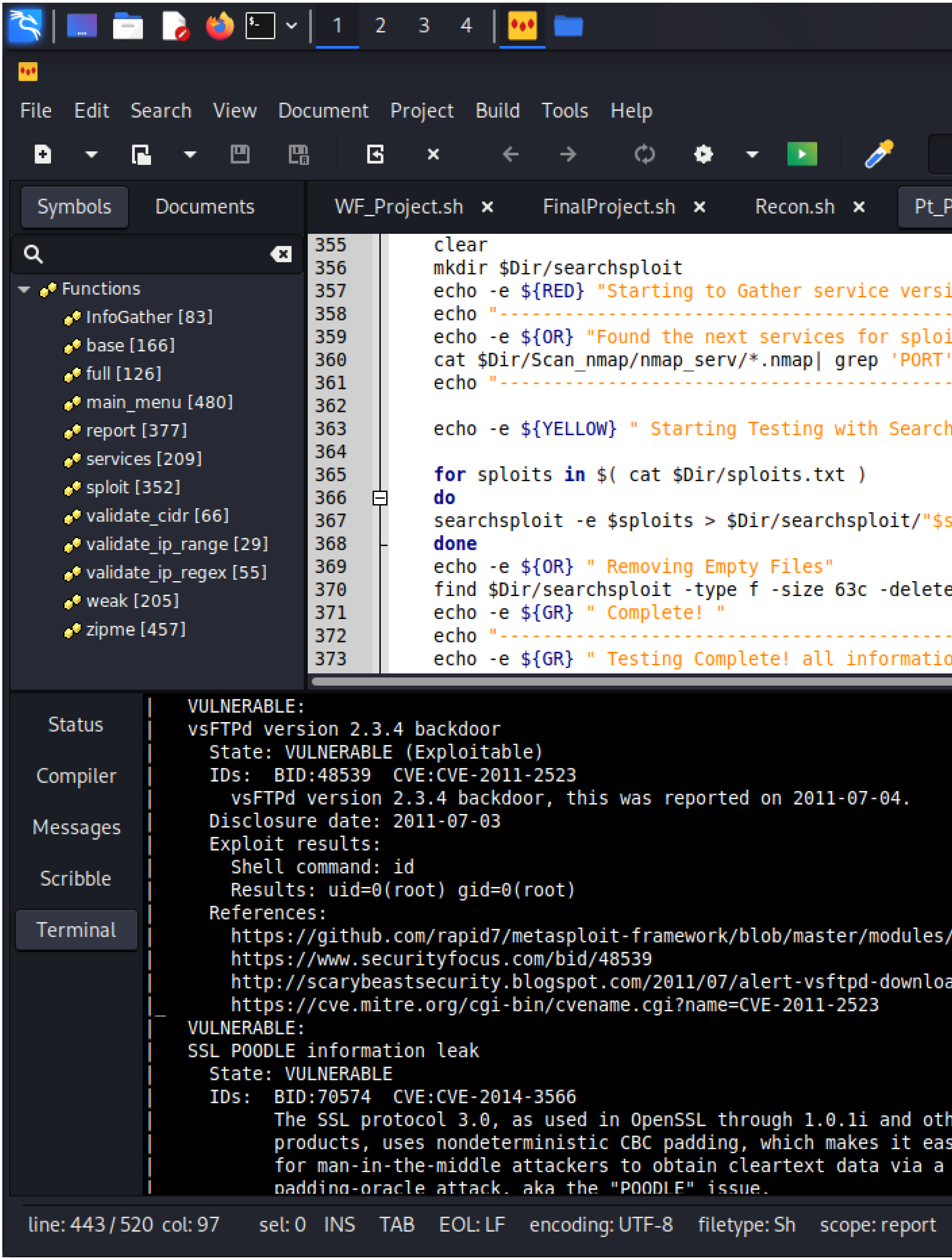
line: 443 / 520 col: 97   sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: report



```
    clear
    mkdir $Dir/searchsploit
    echo -e ${RED} "Starting to Gather service versi
    echo "-----------------------------------------
    echo -e ${OR} "Found the next services for sploi
    cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
    echo "-----------------------------------------

    echo -e ${YELLOW} " Starting Testing with Search

    for sploits in $( cat $Dir/sploits.txt )
    do
    searchsploit -e $sploits > $Dir/searchsploit/"$s
    done
    echo -e ${OR} " Removing Empty Files"
    find $Dir/searchsploit -type f -size 63c -delete
    echo -e ${GR} " Complete! "
    echo "-----------------------------------------
    echo -e ${GR} " Testing Complete! all informatio
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
  Done! Proceeding!
-------------------------------------------------------------------
 Starting Authication Bypass Check! Saving into: test1/Scan_nmap/nmap_auth/
Host script results:
| smb-enum-users:
|_  Domain: METASPLOITABLE; Users: backup, bin, bind, daemon, dhcp, distccd
sync, sys, syslog, telnetd, tomcat55, user, uucp, www-data

Post-scan script results:
| creds-summary:
|   192.168.112.156:
|     8180/nil:
|       tomcat:tomcat - Valid credentials
|_      tomcat:tomcat - Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 30.80 seconds
  Done! Proceeding!
-------------------------------------------------------------------
  Starting Malware Check! Saving Into: test1/Scan_nmap/nmap_malware/192.168
```

line: 443 / 520 col: 97   sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: report



- Functions
  - InfoGather [83]
  - base [166]
  - full [126]
  - main_menu [480]
  - report [377]
  - services [209]
  - sploit [352]
  - validate_cidr [66]
  - validate_ip_range [29]
  - validate_ip_regex [55]
  - weak [205]
  - zipme [457]

```
    clear
    mkdir $Dir/searchsploit
    echo -e ${RED} "Starting to Gather service versi
    echo "--------------------------------------------
    echo -e ${OR} "Found the next services for sploi
    cat $Dir/Scan_nmap/nmap_serv/*.nmap| grep 'PORT'
    echo "--------------------------------------------

    echo -e ${YELLOW} " Starting Testing with Search

    for sploits in $( cat $Dir/sploits.txt )
    do
    searchsploit -e $sploits > $Dir/searchsploit/"$s
    done
    echo -e ${OR} " Removing Empty Files"
    find $Dir/searchsploit -type f -size 63c -delete
    echo -e ${GR} " Complete! "
    echo "--------------------------------------------
    echo -e ${GR} " Testing Complete! all informatio
```

```
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       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://github.com/rapid7/metasploit-framework/blob/master/modules/
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downloa
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and oth
|           products, uses nondeterministic CBC padding, which makes it eas
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
```

line: 443 / 520 col: 97   sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: report