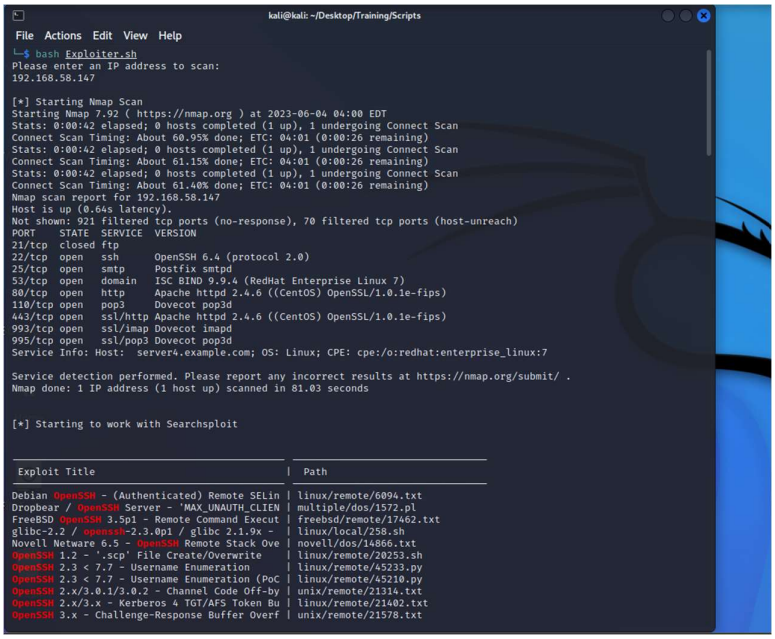
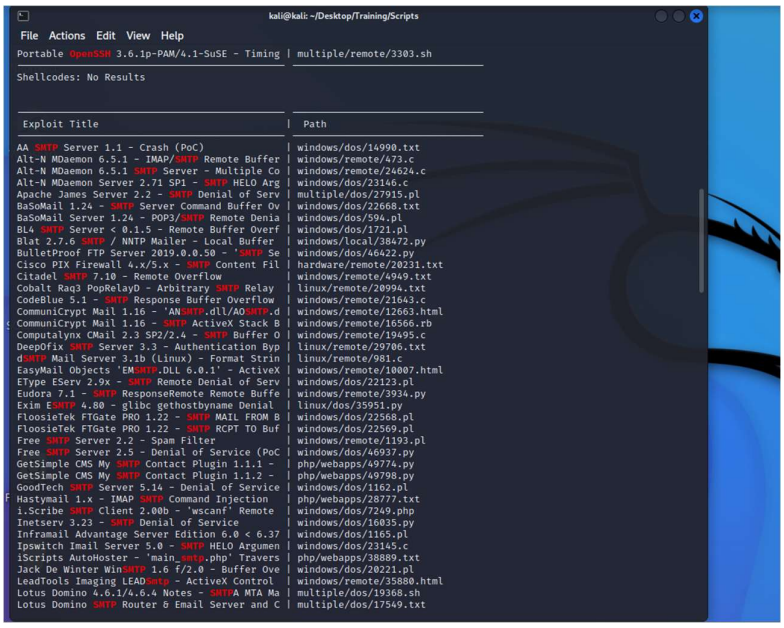
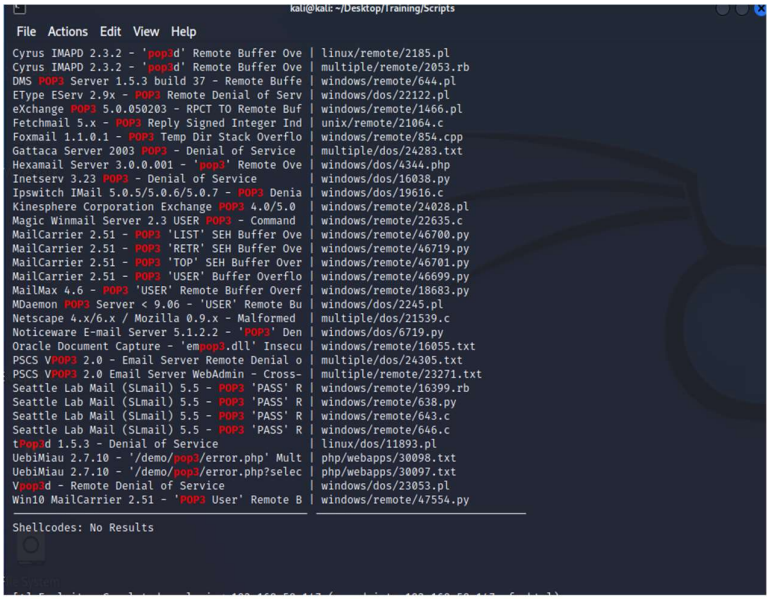
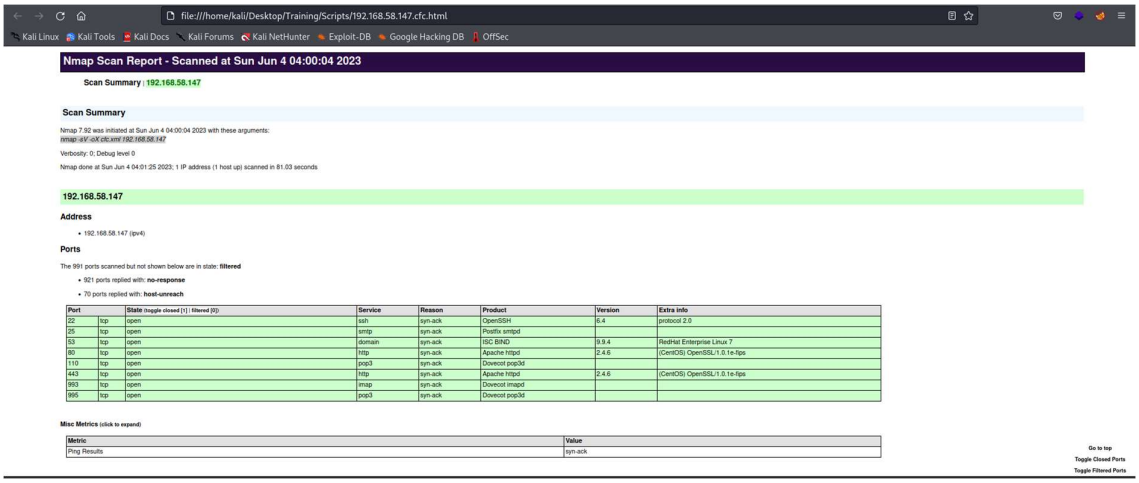
Exploiter.sh

A script that gets the IP from a user, scans the IP using nmap, saves the output into a grepable XML file, uses searchsploit and print out the results to the user.






kali@kali: ~/Desktop/Training/Scripts
File Actions Edit View Help
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Ove | linux/remote/2185.pl
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Ove | multiple/remote/2053.rb
DMS POP3 Server 1.5.3 build 37 - Remote Buffe | windows/remote/644.pl
EType EServ 2.9x - POP3 Remote Denial of Serv | windows/dos/22122.pl
eXchange POP3 5.0.050203 - RPCT TO Remote Buf | windows/remote/1466.pl
Fetchmail 5.x - POP3 Reply Signed Integer Ind | unix/remote/21064.c
Foxmail 1.1.0.1 - POP3 Temp Dir Stack Overflo | windows/remote/854.cpp
Gattaca Server 2003 POP3 - Denial of Service | multiple/dos/24283.txt
Hexamail Server 3.0.0.001 - 'pop3' Remote Ove | windows/dos/4344.php
Inetserv 3.23 POP3 - Denial of Service | windows/dos/16038.py
Ipswitch IMail 5.0.5/5.0.6/5.0.7 - POP3 Denia | windows/dos/19616.c
Kinesphere Corporation Exchange POP3 4.0/5.0 | windows/remote/24028.pl
Magic Winmail Server 2.3 USER POP3 - Command | windows/remote/22635.c
MailCarrier 2.51 - POP3 'LIST' SEH Buffer Ove | windows/remote/46700.py
MailCarrier 2.51 - POP3 'RETR' SEH Buffer Ove | windows/remote/46719.py
MailCarrier 2.51 - POP3 'TOP' SEH Buffer Over | windows/remote/46701.py
MailCarrier 2.51 - POP3 'USER' Buffer Overflo | windows/remote/46699.py
MailMax 4.6 - POP3 'USER' Remote Buffer Overf | windows/remote/18683.py
MDaemon POP3 Server < 9.06 - 'USER' Remote Bu | windows/dos/2245.pl
Netscape 4.x/6.x / Mozilla 0.9.x - Malformed | multiple/dos/21539.c
Noticeware E-mail Server 5.1.2.2 - 'POP3' Den | windows/dos/6719.py
Oracle Document Capture - 'empop3.dll' Insecu | windows/remote/16055.txt
PSCS VPOP3 2.0 - Email Server Remote Denial o | multiple/dos/24305.txt
PSCS VPOP3 2.0 Email Server WebAdmin - Cross- | multiple/remote/23271.txt
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/16399.rb
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/638.py
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/643.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/646.c
tPop3d 1.5.3 - Denial of Service | linux/dos/11893.pl
UebiMiau 2.7.10 - '/demo/pop3/error.php' Mult | php/webapps/30098.txt
UebiMiau 2.7.10 - '/demo/pop3/error.php?selec | php/webapps/30097.txt
Vpop3d - Remote Denial of Service | windows/dos/23053.pl
Win10 MailCarrier 2.51 - 'POP3 User' Remote B | windows/remote/47554.py
Shellcodes: No Results


file:///home/kali/Desktop/Training/Scripts/192.168.58.147.cfc.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Nmap Scan Report - Scanned at Sun Jun 4 04:00:04 2023
Scan Summary | 192.168.58.147
Scan Summary
Nmap 7.92 was initiated at Sun Jun 4 04:00:04 2023 with these arguments:
nmap -sV -oX cfc.xml 192.168.58.147
Verbosity: 0; Debug level 0
Nmap done at Sun Jun 4 04:01:25 2023; 1 IP address (1 host up) scanned in 81.03 seconds
192.168.58.147
Address
192.168.58.147 (ipv4)
Ports
The 991 ports scanned but not shown below are in state: filtered
921 ports replied with: no-response
70 ports replied with: host-unreach
Port | | State (toggle closed [1] | filtered [0]) | Service | Reason | Product | Version | Extra info
22 | tcp | open | ssh | syn-ack | OpenSSH | 6.4 | protocol 2.0
25 | tcp | open | smtp | syn-ack | Postfix smtpd
53 | tcp | open | domain | syn-ack | ISC BIND | 9.9.4 | RedHat Enterprise Linux 7
80 | tcp | open | http | syn-ack | Apache httpd | 2.4.6 | (CentOS) OpenSSL/1.0.1e-fips
110 | tcp | open | pop3 | syn-ack | Dovecot pop3d
443 | tcp | open | http | syn-ack | Apache httpd | 2.4.6 | (CentOS) OpenSSL/1.0.1e-fips
993 | tcp | open | imap | syn-ack | Dovecot imapd
995 | tcp | open | pop3 | syn-ack | Dovecot pop3d
Misc Metrics (click to expand)
Metric | Value
Ping Results | syn-ack
Go to top
Toggle Closed Ports
Toggle Filtered Ports