

Exploiter.sh

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

```
File Actions Edit View Help
~$ bash Exploiter.sh
Please enter an IP address to scan:
192.168.58.147

[*] Starting Nmap Scan
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-04 04:00 EDT
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 60.95% done; ETC: 04:01 (0:00:26 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 61.15% done; ETC: 04:01 (0:00:26 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 61.40% done; ETC: 04:01 (0:00:26 remaining)
Nmap scan report for 192.168.58.147
Host is up (0.645 latency).
Not shown: 921 filtered tcp ports (no-response), 70 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
21/tcp    closed ftp          OpenSSH 6.4 (protocol 2.0)
22/tcp    open  ssh                OpenSSH 6.4 (protocol 2.0)
25/tcp    open  smtp                Postfix smtpd
53/tcp    open  domain             ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
80/tcp    open  http                Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips)
110/tcp   open  pop3                Dovecot pop3d
443/tcp   open  ssl/http            Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips)
993/tcp   open  ssl/imap            Dovecot imapd
995/tcp   open  ssl/pop3            Dovecot pop3d
Service Info: Host: server4.example.com; OS: Linux; CPE: o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.03 seconds

[*] Starting to work with Searchsploit
```

Exploit Title	Path
Debian OpenSSH - (Authenticated) Remote SELIN	linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIEN	multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execut	freebsd/remote/17462.txt
glibc-2.2 / OpenSSH-2.3.0p1 / glibc 2.1.9x -	linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Ove	novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite	linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (Poc)	linux/remote/45210.py
OpenSSH 2.x/0.1/2.0.2 - Channel Code Off-by	linux/remote/21316.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Bu	linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overf	unix/remote/21578.txt

```
File Actions Edit View Help
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing | multiple/remote/3303.sh
Shellcodes: No Results
```

Exploit Title	Path
AA SMTP Server 1.1 - Crash (PoC)	windows/dos/14990.txt
Alt-N MDAemon 6.5.1 - IMAP/SMTP Remote Buffer	windows/remote/473.c
Alt-N MDAemon 6.5.1 SMTP Server - Multiple Co	windows/remote/24624.c
Alt-N MDAemon Server 2.71 SPI - SMTP HELO Arg	windows/dos/22146.c
Apache James Server 2.2 - SMTP Denial of Serv	multiple/dos/27915.pl
BasoMail 1.24 - SMTP Server Command Buffer Ov	windows/dos/22668.txt
BasoMail Server 1.24 - POP3/SMTP Remote Denia	windows/dos/394.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overf	windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer	windows/local/38472.py
BulletProof FTP Server 2019.0.0.50 - 'SMTP Se	windows/dos/46422.py
Cisco PIX Firewall 4.x/5.x - SMTP Content Fil	hardware/remote/20231.txt
Citadel SMTP 7.10 - Remote Overflow	windows/remote/4949.txt
Cobalt Raq3 PopRelayD - Arbitrary SMTP Relay	linux/remote/20994.txt
CodeBlue 5.1 - SMTP Response Buffer Overflow	windows/remote/21643.c
CommuniCrypt Mail 1.16 - 'AN SMTP.dll/AQ SMTP-d	windows/remote/12663.html
CommuniCrypt Mail 1.16 - SMTP ActiveX Stack B	windows/remote/16566.tb
Computalynx CMail 2.3 SP2/2.4 - SMTP Buffer O	windows/remote/19495.c
DeepOfix SMTP Server 3.3 - Authentication Byp	linux/remote/29706.txt
dSMTP Mail Server 2.1b (Linux) - Format Strin	linux/remote/981.c
EasyMail Objects 'EMSMTP.DLL 6.0.1' - ActiveX	windows/remote/10007.html
EType EServ 2.9x - SMTP Remote Denial of Serv	windows/dos/22123.pl
Eudora 7.1 - SMTP ResponseRemote Remote Buffe	windows/remote/3934.py
Exim ESMTP 4.00 - glibc gethostbyname Denial	linux/dos/35951.py
FloosieTek FTGate PRO 1.22 - SMTP MAIL FROM B	windows/dos/22568.pl
FloosieTek FTGate PRO 1.22 - SMTP RCPT TO Buf	windows/dos/22569.pl
Free SMTP Server 2.2 - Spam Filter	windows/remote/1193.pl
Free SMTP Server 2.5 - Denial of Service (PoC)	windows/dos/46937.py
GetSimple CMS My SMTP Contact Plugin 1.1.1 -	php/webapps/49774.py
GetSimple CMS My SMTP Contact Plugin 1.1.2 -	php/webapps/49798.py
GoodTech SMTP Server 5.14 - Denial of Service	windows/dos/1162.pl
Hastymail 1.x - IMAP SMTP Command Injection	php/webapps/28777.txt
i.Scribe SMTP Client 2.00b - 'wscanf' Remote	windows/dos/7249.php
Inetserver 3.23 - SMTP Denial of Service	windows/dos/16035.py
Inframail Advantage Server Edition 6.0 < 6.37	windows/dos/1165.pl
Ipswitch Imaill Server 5.0 - SMTP HELO Argumen	windows/dos/23145.c
IScripts AutoHoster - 'main_smtp.php' Travers	php/webapps/38889.txt
Jack De Winter WinSMTP 1.0 f/2.0 - Buffer Ove	windows/dos/28221.pl
Leadtools Imaging LEADmail - ActiveX Control	windows/remote/35880.html
Lotus Domino 4.6.1/4.6.4 Notes - SMTPA MTA Ma	multiple/dos/19368.sh
Lotus Domino SMTP Router 6 Email Server and C	multiple/dos/17549.txt

```
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/2212.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 5.0.2/5.0.6/5.0.7 - 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 < 0.06 - '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.cf.html

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Nmap Scan Report - Scanned at Sun Jun 4 04:00:04 2023

Scan Summary : 192.168.58.147

Scan Summary

Nmap 7.80 was initiated at Sun Jun 4 04:00:04 2023 with these arguments:
nmap -sV -iL 192.168.58.147

Verbsity: 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 (p4)

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 (tcp reset [1], filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp open	ssh	syn-ack	OpenSSH	8.4	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 OpenSSH 7.5.1-4-RHEL
110	tcp open	pop3	syn-ack	Dovecot pop3d		
443	tcp open	https	syn-ack	Apache httpd	2.4.6	CentOS OpenSSH 7.5.1-4-RHEL
993	tcp open	pop3s	syn-ack	Dovecot pop3d		
995	tcp open	pop3s	syn-ack	Dovecot pop3d		

Mac Metrics (click to expand)

Metric	Value
Ping Periods	101-ack

Go to top

Toggle Closed Ports

Toggle Filtered Ports